PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-063147
(43)Date of publication of application : 28.02.2002

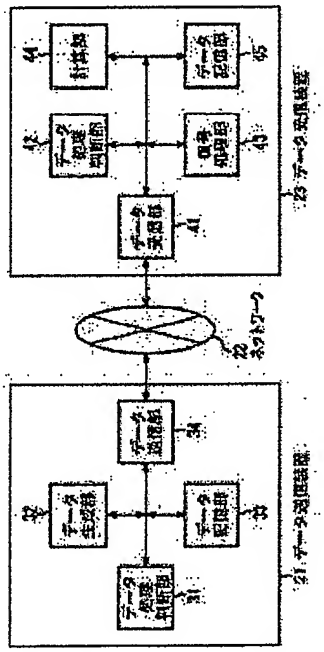
(51)Int.Cl. G06F 15/177
H04L 9/10

(21)Application number : 2000-247230
(22)Date of filing : 17.08.2000

(71)Applicant : SONY CORP
(72)Inventor : MUTO AKIHIRO

(54) DEVICE FOR PROCESSING INFORMATION, METHOD FOR THE SAME AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To ensure processing performance for decoding enciphered contents data.
SOLUTION: A data receiver 23 for receiving and decoding contents data transmitted from a data transmitter 21 confirms the contents of meta data, in which information related with the encipherment of the contents data is described, before processing the contents data. A decoding processing part 43 compares the processing contents requested by the meta data with own processing performance, and when the requested processing cannot be achieved is decided when the decoding is performed by the decoding processing part 43 alone, the decoding processing part 43 requests a calculating part 44 to conduct dispersion processing of the contents data. The decoding processing part 43 receives and conducts the dispersion and decoding of the contents data, when the authentication of the dispersion processing is established with the calculating part 44, which is requested to conduct the dispersion processing.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－63147
（P2002－63147A）
(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/177	６７４	Ｇ０６Ｆ　15/177	６７４Ａ	５Ｂ０４５
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数４　ＯＬ　（全 27 頁）

(21)出願番号　特願2000－247230(P2000－247230)

(22)出願日　平成12年８月17日(2000.8.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

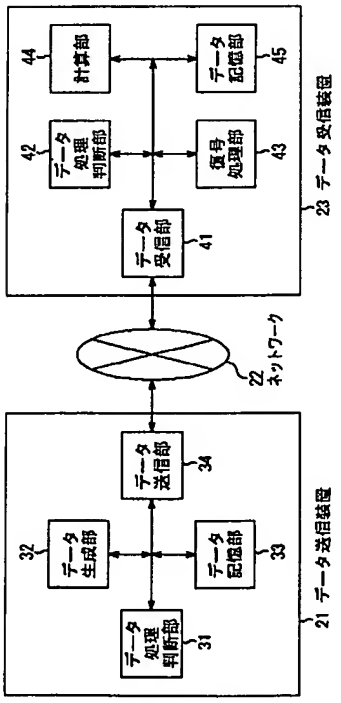
(72)発明者　武藤　明宏
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5B045 GG01
5J104 AA09 AA32 LA01 LA05 LA06
PA07 PA11 PA14

(54)【発明の名称】　情報処理装置、情報処理方法、並びに記録媒体

(57)【要約】
【課題】　暗号化されたコンテンツデータを復号する処理能力を確保する。
【解決手段】　データ送信装置２１から送信されるコンテンツデータを受信して復号処理するデータ受信装置２３は、コンテンツデータを処理する前に、コンテンツデータの暗号化に関する情報が記述されているメタデータの内容を確認する。復号処理部４３は、メタデータにより要求される処理内容と、自分自身の処理能力を比較し、復号処理部４３が単独で復号処理を行ったのでは、要求される処理を行うことができないと判定した場合、計算部４４に対して、コンテンツデータを分散して処理することを要求する。復号処理部４３は、分散処理を要求した計算部４４との間で分散処理の認証が成立した場合、コンテンツデータを受信し、分散して復号処理する。



1

【特許請求の範囲】

【請求項１】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、前記受信手段により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識手段と、

前記認識手段により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較手段と、

前記比較手段により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理手段とを含むことを特徴とする情報処理装置。

【請求項２】　前記他のデータ処理部の前記データ処理が、前記所定のデータ処理部が分散処理を委託する処理要求に基づいて実行されているか否かを判断する判断手段をさらに含むことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、

前記認識ステップの処理により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、

前記比較ステップの処理により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする情報処理方法。

【請求項４】　コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、

前記受信ステップの処理により受信された前記特徴情報から、前記コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、

前記認識ステップの処理により認識された前記データ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、

前記比較ステップの処理により比較された自分自身の処理能力が、前記データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部に前記データ処理を委託し、前記コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とするコンピュータが読みとり可能なプログラムが記録されている記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、並びに記録媒体に関し、特に、暗号化されたコンテンツデータのデータ処理を、他のデータ処理部と分散して処理することにより、システム毎に設計したハードウエアを用いることなく、迅速にデータを処理することを可能にした情報処理装置、情報処理方法、並びに記録媒体に関する。

【０００２】

【従来の技術】近年、コンテンツデータをネットワークを介して配信する配信システムが構築されている。配信されるコンテンツデータは、データの改竄を防ぐため、暗号化や、ディジタル署名を付加するなどの処理が施されている。暗号化されたコンテンツデータは、利用者の端末により復号処理され、利用者はそれを利用することができる。

【０００３】暗号化技術の安全性は、復号する際の処理の難しさに依存しているため、暗号化技術の高度化にともなって、コンテンツデータを利用する利用者の端末には、より処理能力の高い端末が要求されるようになっている。

【０００４】そこで、処理能力を確保するために、利用者端末に復号処理専用のLSI（LargeScale Integration）を配置することが考えられる。図１は、復号処理専用のLSI（以下、復号LSIと称する）の構成例を示している。

【０００５】復号LSI１は、復号LSI１の外部に配置されるコントロールマイクロコンピュータ（以下、コントロールマイコンと略称する）２から転送される指令により復号処理を行う。復号処理には、暗号化されたコンテンツデータを復号する処理の他に、コンテンツデータに付加されているディジタル署名を検証する処理が含まれる。復号LSI１が処理した結果は、復号LSI１の外部に配置される外部メモリ３に記憶される。

【０００６】復号LSI１は、通信インタフェース１１、コントロールユニット１２、RAM（Random Access Memory）１３、メモリコントローラ１４、フラッシュメモリ１５、べき乗演算器１６、ハッシュ値演算器１７から構成される。

【０００７】コントロールマイコン２から転送される指令は、通信インタフェース１１を介してコントロールユニット１２に伝えられる。コントロールユニット１２は、べき乗演算器１６およびハッシュ値演算器１７などを補助的に用いつつ、復号LSI１の全体の動作を制御し、暗号化されているデータの復号処理、およびディジタル署名の検証処理などを行う。

【０００８】RAM１３には、コントロールユニット１２が利用するプログラムが記憶されている。

【０００９】メモリコントローラ１４は、外部メモリ３に対するデータの読み書きを制御する。

【００１０】フラッシュメモリ１５には、コントロールユニット１２の指令によりべき乗演算器１６、およびハッシュ値演算器１７が演算した結果や、処理に必要なデータが、適宜、記憶される。

【００１１】利用者が使用する端末に、上述したような復号LSI１を配置することにより、コンテンツデータの復号処理能力を確保することが可能となる。

【００１２】

【発明が解決しようとする課題】しかしながら、利用者端末に復号LSI１（ハードウエア）を設置する場合、暗号化されたコンテンツデータの復号処理能力は、暗号化のセキュリティレベルに応じて計算量が異なるため、最大の負荷を処理することができるように復号LSI１を構成する必要がある。その結果、コスト高となる課題があった。また、処理能力を変更する必要が生じた場合、LSIを設計し直す必要があるため、バージョンアップ等の変更が実質的に困難になる課題があった。

【００１３】本発明はこのような状況に鑑みてなされたものであり、暗号化されたコンテンツデータを利用者端末において復号する場合に、システム毎に設計したハードウエアを利用することなく、低コストで、かつ、比較的容易に機能を変更できるシステムを実現できるようにするものである。

【００１４】

【課題を解決するための手段】本発明の情報処理装置は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信手段と、受信手段により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識手段と、認識手段により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較手段と、比較手段により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理手段とを含むことを特徴とする。

【００１５】本発明の情報処理装置は、前記他のデータ処理部のデータ処理が、所定のデータ処理部が分散処理を委託する処理要求に基づいて実行されているか否かを判断する判断手段をさらに含むようにすることができる。

【００１６】本発明の情報処理方法は、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、認識ステップの処理により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、比較ステップの処理により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする。

【００１７】本発明の記録媒体のプログラムは、コンテンツデータと、その特徴に関する情報が記述されている特徴情報を受信する受信ステップと、受信ステップの処理により受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識する認識ステップと、認識ステップの処理により認識されたデータ処理に要求される処理能力と、自分自身の処理能力を比較する比較ステップと、比較ステップの処理により比較された自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理を委託し、コンテンツデータを分散処理する分散処理ステップとを含むことを特徴とする。

【００１８】本発明の情報処理装置、情報処理方法、および記録媒体のプログラムにおいては、コンテンツデータと、その特徴に関する情報が記述されている特徴情報が受信され、受信された特徴情報から、コンテンツデータのデータ処理に要求される処理能力が認識される。また、認識されたデータ処理に要求される処理能力と、自分自身の処理能力が比較され、自分自身の処理能力が、データ処理に要求される処理能力を充足していないと判断された場合、所定のデータ処理部だけでなく、他のデータ処理部にデータ処理が委託され、コンテンツデータが分散処理される。

【００１９】

【発明の実施の形態】図２は、本発明を適用したデータ処理システムの構成例を示すブロック図である。データ送信装置２１により生成され、暗号化されたコンテンツデータは、ネットワーク２２を介してデータ受信装置２３に送信される。

【００２０】データ送信装置２１は、データ処理判断部３１、データ生成部３２、データ記憶部３３、およびデータ送信部３４から構成される。

【００２１】データ処理判断部３１は、データ送信装置２１の全体の動作を制御する。データ生成部３２は、所定の方法により提供されたコンテンツデータを暗号化したり、ディジタル署名を生成する（以下、コンテンツデータの暗号化処理、およびディジタル署名の生成処理をまとめて暗号関連処理と称する）。また、データ生成部３２は、コンテンツデータの暗号化に関するデータなどが記述されているメタデータを生成する。データ記憶部３３は、データ生成部３２により生成されたコンテンツデータおよびメタデータを記憶する。データ送信部３４は、データ受信装置２３からの要求に応じて、データ記

憶部３３に記憶されているメタデータおよびコンテンツデータを送信する。

【００２２】ネットワーク２２は、データ送信装置２１およびデータ受信装置２３の間で送受信されるデータの伝送路であり、例えば、インターネット、電話回線網、ケーブルテレビジョン放送網、衛星を介したディジタルテレビジョン放送網等により構成される。

【００２３】データ受信装置２３は、データ受信部４１、データ処理判断部４２、復号処理部４３、計算部４４、およびデータ記憶部４５より構成される。

【００２４】データ受信部４１は、データ送信装置２１から送信されたメタデータおよびコンテンツデータを受信する。データ処理判断部４２は、データ受信装置２３の全体の動作を制御する。復号処理部４３は、データ受信部４１により受信されたコンテンツデータが暗号化されている場合にはコンテンツデータを復号し、ディジタル署名が付加されている場合には、ディジタル署名の検証などの処理を行う（以下、コンテンツデータの復号処理、およびディジタル署名の検証処理をまとめて復号関連処理と称する）。計算部４４は、データ処理判断部４２の指令を受けて、演算処理機能を提供する。データ記憶部４５は、データ受信部４１により受信されたコンテンツデータ、および復号処理部４３により復号され、かつディジタル署名が検証されたコンテンツデータを記憶する。

【００２５】次に、データ送信装置２１が送信するメタデータおよびコンテンツデータを、データ受信装置２３が受信し、処理する一連の処理について、図３乃至図５のフローチャートを参照して説明する。

【００２６】図３は、データ送信装置２１の処理を説明するフローチャートである。ステップS１において、データ生成部３２は、外部から所定の方法により提供されるアナログデータまたはディジタルデータを取得し、コンテンツデータを作成する。データ生成部３２は、ネットワーク２２を介してデータ受信装置２３に対して送信することが可能な形式に圧縮し、暗号関連処理を施して、コンテンツデータを作成する。

【００２７】また、データ生成部３２は、メタデータを生成する。メタデータには、送信されるコンテンツデータの特徴、コンテンツデータの暗号関連処理に関する情報である暗号関連情報が記述される。コンテンツデータの特徴には、例えば、コンテンツデータの制作者、制作時期、制作者を識別する制作者ID、コンテンツデータの利用形態、コンテンツデータ利用形態毎の料金、コンテンツデータの再生時間、コンテンツデータの圧縮方法、総データ量、データの転送速度などが含まれる。また、コンテンツデータの暗号関連情報には、例えば、暗号化アルゴリズム、ディジタル署名の生成アルゴリズム、データ単位が含まれる。これらの具体例については後述する。

【００２８】ステップS２において、データ記憶部３３は、ステップS１の処理でデータ生成部３２により作成されたコンテンツデータおよびメタデータを記憶する。

【００２９】ステップS３において、データ処理判断部３１は、データ受信装置２３からメタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。データ処理判断部３１によりメタデータの送信が要求されたと判定された場合、処理はステップS４に進む。

【００３０】ステップS４において、データ送信部３４は、データ記憶部３３に記憶されているメタデータを、ネットワーク２２を介してデータ受信装置２３に送信する。後述するように、メタデータを受信したデータ受信装置２３は、メタデータに記述されている情報を分析し、コンテンツデータの処理を準備する。メタデータに記述されているコンテンツデータの情報に応じて、コンテンツデータを処理する準備が完了した場合、データ受信装置２３は、コンテンツデータの送信をデータ送信装置２１に要求する。

【００３１】そこで、ステップS５において、データ処理判断部３１は、データ受信装置２３からコンテンツデータの送信が要求されたか否かを判定する。

【００３２】ステップS５において、データ処理判断部３１によりデータ受信装置２３からコンテンツデータの送信が要求されていないと判定された場合、データ処理判断部３１は、データ受信装置２３が、コンテンツデータの処理の準備が完了していないと認識し、コンテンツデータの送信が要求されるまで待機する。

【００３３】ステップS５において、データ処理判断部３１が、データ受信装置２３からコンテンツデータの送信が要求されたと判定した場合、処理はステップS６に進み、データ送信部３４は、データ記憶部３３に記憶されているコンテンツデータを、ネットワーク２２を介してデータ受信装置２３に対して送信する。

【００３４】図４および図５は、データ受信装置２３の処理を説明するフローチャートである。ステップS１１において、データ処理判断部４２は、データ受信装置２３を管理する利用者からコンテンツデータの受信の指令が入力された場合、データ送信装置２１に対して、そのコンテンツデータに対応するメタデータの送信を要求する。

【００３５】ステップS１２において、データ受信部４１は、データ送信装置２１から送信されてきたメタデータを、ネットワーク２２を介して受信する。データ受信部４１が受信したメタデータは、データ処理判断部４２に転送され、データ処理判断部４２により記述されている内容が分析される。

【００３６】ステップS１３において、データ処理判断部４２は、メタデータに記述されているコンテンツデータの情報から、送信されてくるコンテンツデータは、暗

号関連処理が施されているか否かを判定する。

【００３７】ステップＳ１３において、データ処理判断部４２は、送信されてくるコンテンツデータには、暗号関連処理が施されていないと判定した場合、処理はステップＳ１４に進み、データ処理判断部４２は、データ送信装置２１に対して、コンテンツデータの送信を要求する。

【００３８】ステップＳ１５において、データ受信部４１は、データ送信装置２１から、ネットワーク２２を介して送信されたコンテンツデータを受信する。データ受信装置２３を管理する利用者がデータ受信部４１により受信されたコンテンツデータを利用する場合、コンテンツデータは復号関連処理を行う必要がないため、データ記憶部４５は、コンテンツデータを記憶し、データ受信装置２３を管理する利用者から要求があるまで保持する。

【００３９】一方、ステップＳ１３において、データ処理判断部４２は、メタデータに記述されている内容から、送信されてくるコンテンツデータは暗号関連処理が施されているデータであると判定した場合、処理はステップＳ１６に進む。

【００４０】ステップＳ１６において、データ処理判断部４２は、コンテンツデータの暗号関連処理に関する情報である暗号関連情報を含むメタデータを復号処理部４３に通知する。暗号関連情報には、コンテンツデータの暗号化アルゴリズム、ディジタル署名のアルゴリズムおよびデータ単位が記述されている。復号処理部４３は、コンテンツデータの暗号関連情報に基づいて、データ受信部４１がコンテンツデータを受信した場合のコンテンツデータの復号関連処理を準備する。なお、データ処理判断部４２により転送される暗号関連情報は、処理内容の漏洩、処理内容の改竄を防ぐために、さらに暗号関連処理が施されている場合があるが、ここでは、暗号関連情報には暗号関連処理が施されていないものとして説明する。

【００４１】ステップＳ１７において、復号処理部４３は、データ受信部４１により受信されたコンテンツデータの復号関連処理のうちの少なくとも一部を、他の処理部に委託する（分散処理する）必要があるか否かを判定する。この判定は、復号処理部４３が、コンテンツデータの暗号化アルゴリズムに対応しているか否か、または、復号処理部４３の暗号処理能力により、要求される時間内に復号関連処理を完了することが可能であるか否かなどを基準として行われる。

【００４２】ステップＳ１７において、復号処理部４３が、コンテンツデータの分散処理は必要でないと判定した場合、すなわち、コンテンツデータの復号関連処理は復号処理部４３が単独で行うことが可能であると判定した場合、処理はステップＳ１８に進む。

【００４３】ステップＳ１８において、復号処理部４３から、コンテンツデータの復号関連処理の準備が完了した旨の通知を受けたデータ処理判断部４２は、データ送信装置２１に対して、コンテンツデータの送信を要求する。

【００４４】ステップＳ１９において、データ受信部４１はコンテンツデータを受信する。受信されたコンテンツデータは、復号処理部４３に転送され、復号処理部４３は、単独で、コンテンツデータの復号関連処理を行う。復号関連処理が行われ、利用することが可能となったデータは、データ記憶部４５に記憶される。

【００４５】一方、ステップＳ１７において、復号処理部４３は、コンテンツデータを単独で復号関連処理を行うことができず、分散処理が必要であると判定した場合、処理はステップＳ２０に進み、復号処理部４３は分散処理の委託形式を決定し、決定した委託形式の情報とともに、コンテンツデータの分散処理が必要であるとデータ処理判断部４１に通知する。

【００４６】分散処理の委託形式には、一部の復号関連処理を委託する形式、または全ての復号関連処理を委託する形式などがある。一部の復号関連処理を委託する形式は、例えば、コンテンツデータにディジタル署名が付加されており、復号処理部４３が、単独で復号処理とディジタル署名の検証処理を行ったのでは、要求されている時間内に処理を完了することができない場合に、一方の処理を委託する形式である。また、全ての復号関連処理を委託する形式は、復号処理部４３が、コンテンツデータの暗号化アルゴリズムに対応していない場合に委託する形式である。なお、これらの委託形式は、データ送信装置２１においてメタデータに記述することにより、または、データ受信装置２３において予め設定することにより決定することが可能である。

【００４７】ステップＳ２１において、データ処理判断部４２は、ステップＳ２０で復号処理部４３から通知された分散処理の委託形式などの情報に基づいて、コンテンツデータの分散処理先を検索する。分散処理先の候補は、データ処理判断部４２にリスト化されて予め与えられている。

【００４８】ステップＳ２１の処理の結果、データ処理判断部４２は、コンテンツデータの分散処理先として例えば計算部４４を検出し、ステップＳ２２において、計算部４４に対して、コンテンツデータの分散処理を要求する。

【００４９】ステップＳ２３において、復号処理部４３と、データ処理判断部４２によりコンテンツデータの分散処理を要求された計算部４４の間で、相互認証が行われる。この相互認証により、復号処理部４３は、計算部４４が分散処理した処理結果の出力先を指定する。復号処理部４３は、計算部４４に対して処理結果の出力先を例えば、データ記憶装置４５と指定する。

【００５０】ステップＳ２４において、復号処理部４３

は、計算部４４と相互認証が成立したか否かを判定する。

【００５１】ステップS２４の処理の結果、復号処理部４３が計算部４４と相互認証が成立していないと判定した場合、復号処理部４３は、コンテンツデータの復号関連処理が不可能であることを認識する。このとき、復号処理部４３は、コンテンツデータの復号関連処理は不可能であることをデータ処理判断部４２に通知する。その後、データ処理判断部４２により処理は終了される。

【００５２】ステップS２４において、復号処理部４３が、計算部４４との相互認証が成立し、コンテンツデータの分散処理の準備が完了したと判定した場合、処理はステップS２５に進む。

【００５３】ステップS２５において、復号処理部４３からコンテンツデータの分散処理の準備が完了した旨の通知を受け取ったデータ処理判断部４２は、データ送信装置２１にコンテンツデータの送信を要求する。

【００５４】ステップS２６において、データ受信部４１は、ネットワーク２２を介してデータ送信装置２１から送信されてくるコンテンツデータを受信する。

【００５５】ステップS２７において、データ受信部４１が受信したコンテンツデータは、データ処理判断部４２を経由して復号処理部４３に転送され、復号処理部４３は計算部４４に対して、ステップS２２でデータ処理判断部４２が要求した委託形式に基づいて、コンテンツデータの分散処理を指令する。

【００５６】ステップS２８において、復号処理部４３は、ステップS２３で計算部４４に通知した分散処理の出力先から、コンテンツデータの分散処理の結果を取得することができたか否かを判定する。復号処理部４３は、分散処理の結果を取得することができないと判定した場合、ステップS２９に進み、コンテンツデータは不正なデータであると認識し、データ処理判断部４２に通知する。その後、データ処理判断部４２は、データ受信装置２３の利用者に対して不正があったことを通知するとともに、処理を終了する。

【００５７】ステップS２８において、復号処理部４３は、計算部４４に対して指定した出力先に、コンテンツデータの分散処理の結果が指定通りに転送されていると判定した場合、処理はステップS３０に進む。

【００５８】ステップS３０において、復号処理部４３による復号関連処理の結果は、計算部４４による分散処理の処理結果とともに、データ記憶部４５に記憶される。

【００５９】図６は、本発明を適用したコンテンツ配信システムの構成を示す図である。コンテンツプロバイダ５１は、コンテンツサーバ５２を管理しており、コンテンツデータおよびメタデータを作成する。コンテンツプロバイダ５１が作成したコンテンツデータおよびメタデータは、サービスプロバイダ５３が管理するサービスサーバ５４に供給される。コンテンツデータは、映画、音楽などのディジタルデータであり、メタデータにはそれらのデータに関する情報が記述される。

【００６０】サービスプロバイダ５３は、ネットワーク２２を介して、契約者である利用者５５に対してコンテンツデータおよびメタデータを送信する。

【００６１】利用者５５は、サービスプロバイダ５３から送信されたコンテンツデータおよびメタデータを、自らが操作する利用者端末５６において利用する。

【００６２】決済センタ５７は、決済サーバ５８を管理しており、利用者５５に対してコンテンツデータの使用権情報を発行するとともに、使用権情報の代金の決済処理を行う。また、決済センタ５７は、利用者５５から支払われた代金を、コンテンツプロバイダ５１と、サービスプロバイダ５３の間で予め設定された契約に基づいて分配する。

【００６３】図７は、コンテンツサーバ５２の構成例を示すブロック図である。コンテンツサーバ５２は、データキャプチャ装置７１、データ編集装置７２、メタデータ生成装置７３、データ暗号化装置７４、データ記憶装置７５、およびデータ送信装置７６より構成される。

【００６４】データキャプチャ装置７１は、外部から取り込んだデータを、コンテンツサーバ５２の各装置が処理できるデータ形式に変換する。

【００６５】データ編集装置７２は、データキャプチャ装置７１から転送されたデータから、利用者５５に提供するコンテンツデータを作成する装置である。また、データ編集装置７２は、メタデータ生成装置７３が生成したメタデータをコンテンツデータに付加する。

【００６６】データ暗号化装置７４は、データ編集装置７２から転送されたコンテンツデータおよびメタデータに暗号関連処理を施す。

【００６７】データ記憶装置７５は、データ暗号化装置７４により暗号関連処理が施されたメタデータおよびコンテンツデータを記憶し、必要に応じてデータ送信装置７６に転送する。

【００６８】データ送信装置７６は、サービスプロバイダ５３が管理するサービスサーバ５４にコンテンツデータを送信する。なお、具体的な各装置の処理については、図１５のフローチャートを参照して後述する。

【００６９】図８は、データ暗号化装置７４の詳細な構成例を示すブロック図である。データ暗号化装置７４は、入出力インタフェースブロック９１、データ処理判断ブロック９２、データ記憶ブロック９３、乱数生成ブロック９４、および暗号化処理ブロック９５から構成される。さらに、暗号化処理ブロック９５は、暗号化処理サブブロック９６、ディジタル署名生成サブブロック９７、およびハッシュ値計算サブブロック９８より構成される。

【００７０】入出力インタフェースブロック９１は、デ

ータ編集装置７２から供給されるメタデータおよびコンテンツデータを、データ処理判断ブロック９２に転送する。

【００７１】データ処理判断ブロック９２は、データ暗号化装置７４の全体の動作を制御する。

【００７２】データ記憶ブロック９３は、暗号化処理ブロック９５において、暗号関連処理が施されたメタデータおよびコンテンツデータや、処理に必要なデータを、適宜、記憶する。

【００７３】乱数生成ブロック９４は、データ処理判断ブロック９２からの指令により乱数を生成し、暗号化処理ブロック９５に供給する。乱数生成ブロック９４が生成する乱数は、暗号化アルゴリズムであるDES（Data Encryption Standard）、RSA（Rivest-Shamir-Adleman scheme）などの共通鍵暗号方式で暗号関連処理する場合の鍵として利用される。

【００７４】暗号化処理ブロック９５は、コンテンツデータの暗号化およびディジタル署名の生成処理を行う。この暗号化処理ブロック９５の暗号化処理サブブロック９６は、DES、RSAなどの暗号化アルゴリズムによりコンテンツデータの暗号化処理を行う。

【００７５】ディジタル署名生成サブブロック９７は、DSA（Digital Signature Algorithm）などによるディジタル署名の生成アルゴリズムによりディジタル署名を生成する。ディジタル署名は、データの改竄のチェックおよびデータの制作者を認証するためのデータである。

【００７６】ハッシュ値計算サブブロック９８は、ハッシュ関数による計算を行う。ハッシュ関数は、送信するデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、出力であるハッシュ値から入力データを復元することが難しく、また、同一の出力結果のハッシュ値を持つ入力データを探し出すことが困難である（一方向である）特徴を有する。

【００７７】ここで、ディジタル署名の生成および検証について説明する。ディジタル署名の生成者は、送信するデータから特定のアルゴリズムを用いて、メッセージダイジェストを作成する（ハッシュ値計算サブブロック９８により、送信するデータに、ハッシュ関数を適用し、メッセージダイジェストを作成する）。ディジタル署名の生成者は、自分の秘密鍵（乱数生成ブロック９４により生成された乱数）を使って、このメッセージダイジェストと送信するデータの全文を暗号化し、利用者に送信する。

【００７８】一方、データの利用者は、データを受信し、ディジタル署名の生成者が提供する公開鍵を利用して、暗号化されているデータの全文、およびメッセージダイジェストを復号処理する。次に、データの利用者は復号したデータの全文から、ディジタル署名の生成者と同一の方式（同一のハッシュ関数）でメッセージダイジェストを作成する。生成されたメッセージダイジェストと受信されたメッセージダイジェストを比較することにより、ディジタル署名の検証が行なわれる。すなわち、データの送信者から送信され、受信者が復号したメッセージダイジェストと、受信者が復号したデータの全文から、送信者と同一の方式により作成したメッセージダイジェストが等しければ、そのデータは改竄などの不正な処理が行われていないことを表す。

【００７９】なお、データ暗号化装置７４において、説明の便宜上、暗号化処理サブブロック９６、およびディジタル署名生成サブブロック９７は暗号関連処理を行うことが可能であるとしたが、通常は、復号関連処理も行うことが可能である。すなわち、暗号化処理サブブロック９６はデータの暗号化および復号が可能であるし、ディジタル署名生成サブブロック９７はディジタル署名の生成および検証が可能である。

【００８０】さらに、後述する図１３の暗号化処理ブロック１６３に配置されている暗号化処理部１８６を構成するサブブロックも、データ暗号化装置７４を構成するサブブロックと同様に、復号関連処理だけでなく暗号関連処理を実行することができる。また、サービスサーバ５４に配置されているデータ暗号化装置１１４も上述したコンテンツサーバ５２に配置されているデータ暗号化装置７４、および復号処理ブロック１６３と同様に、復号関連処理だけでなく暗号関連処理を実行することができる。これにより、それぞれの装置間で送受信されるデータに、改竄などの不正な処理が行われることを防ぐことが可能となる。

【００８１】上述したような暗号関連処理が施されたコンテンツデータおよびメタデータは、サービスプロバイダ５３が管理するサービスサーバ５４に送信される。

【００８２】図９は、サービスサーバ５４の構成例を示すブロック図である。サービスサーバ５４は、データ送受信装置１１１、データ編集装置１１２、メタデータ生成装置１１３、データ暗号化装置１１４、コンテンツプロモーションサーバ１１５、およびデータ記憶装置１１６より構成される。

【００８３】データ送受信装置１１１は、コンテンツサーバ５２から送信されるコンテンツデータおよびメタデータを受信する。また、データ送受信装置１１１は、利用者端末５６に対し、ネットワーク２２を介してコンテンツデータおよびメタデータを送信する。データ送受信装置１１１は、コンテンツデータおよびメタデータを送信するタイミングを判断する。送信するタイミングは、例えば、利用者５５からの要求に応じて送信する場合や、メタデータに記述されているタイミングで送信する場合などがある。

【００８４】データ編集装置１１２は、サービスサーバ５４の各装置で処理されたデータを編集し、利用者５５に提供する形態にデータを編集する。

【００８５】メタデータ生成装置１１３は、メタデータを生成する。メタデータ生成装置１１３が生成するメタデータには、サービスプロバイダ５３がコンテンツデータを利用者５５に提供する際に、サービスプロバイダ５３が利用者５５に対して通知する情報が記述される。

【００８６】データ暗号化装置１１４は、メタデータ生成装置１１３が生成したメタデータにディジタル署名を生成するなどの暗号関連処理を行う。データ暗号化装置１１４の詳細な構成は、図７に示すコンテンツサーバ５２のデータ暗号化装置７４（図８）の構成と同様である。

【００８７】コンテンツプロモーションサーバ１１５は、サービスプロバイダ５３が利用者５５に提供するコンテンツの一覧情報を作成するとともに、ディスカウント情報などを利用者５５の要求に応じて提供する。コンテンツプロモーションサーバ１１５は、WWWサーバとして設置され、利用者５５は利用者端末５６に装備されているブラウザを利用することにより、コンテンツプロモーションサーバ１１５が提供するサービスを受けることができる。さらに、コンテンツプロモーションサーバ１１５は、利用者５５からの電話による問い合わせに対応できるようにもなっている。

【００８８】データ記憶装置１１６は、データ編集装置１１２で編集されたデータを記憶し、利用者５５からの要求に応じて、データ送受信装置１１１に対してコンテンツデータおよびメタデータを転送する。なお、具体的な各装置の処理については、図１８のフローチャートを参照して後述する。

【００８９】図１０は、決済センタ５７が管理している決済サーバ５８の構成例を示すブロック図である。決済サーバ５８は、データ送受信装置１３１、ライセンス装置１３２、ユーザ管理装置１３３、著作権管理装置１３４、課金装置１３５、および決済装置１３６より構成される。

【００９０】データ送受信装置１３１は、利用者端末５６から、ネットワーク２２を介して通知されるコンテンツデータの使用権の購入要求情報を受信するとともに、コンテンツプロバイダ５１およびサービスプロバイダ５３に対して、利用者５５から回収した代金の課金情報を送信する。

【００９１】ライセンス装置１３２は、利用者５５からコンテンツデータの使用権購入が要求された場合、使用権情報の発行処理を行う。

【００９２】ユーザ管理装置１３３は、サービスプロバイダ５３から、コンテンツデータの提供を受ける契約をしている利用者５５、およびその利用者５５が操作する利用者端末５６の情報を管理する。利用者５５および利用者端末５６の情報には、利用者端末５６に含まれるセットトップボックスの契約日、契約条件、サービスの利用情報などが含まれる。

【００９３】著作権管理装置１３４は、コンテンツデータの著作権の他、サービスプロバイダ５３から提供される利用者５５が利用可能なコンテンツデータの利用形態、および利用者５５によるコンテンツデータの購入履歴などを管理する。

【００９４】課金装置１３５は、コンテンツデータの使用権情報の料金情報を管理するとともに、利用者５５に対して、課金情報を通知する。

【００９５】決済装置１３６は、課金装置１３５から決済処理の要求をうけて、決済処理を行う。具体的な決済方法には、クレジットカードによる決済方法、プリペイド型の電子マネーによる決済方法が含まれる。なお、決済サーバ５８の使用権情報の発行処理については、図２０および２１のフローチャートを参照して後述する。

【００９６】図１１は、利用者５５が管理する利用者端末５６の構成例を示すブロック図である。利用者端末５６は、セットトップボックス１５１（以下、適宜、STB１５１と称する）、およびデータ再生装置１５２より構成される。

【００９７】STB１５１は、ネットワーク２２を介して、サービスサーバ５４、および決済サーバ５８との間でデータの送受信を行う。STB１５１の詳細な構成例は図１２に示す。

【００９８】データ再生装置１５２は、サービスサーバ５４から提供され、STB１５１が処理したコンテンツデータを再生する装置である。データ再生装置１５２は、例えば、テレビジョン受像機、パーソナルコンピュータなどの電子機器により構成される。

【００９９】図１２は、セットトップボックス１５１の構成例を示すブロック図である。STB１５１は、データ送受信ブロック１６１、コントローラ１６２、暗号化処理ブロック１６３、フラッシュメモリ１６４、および外部RAM（Random Access Memory）１６５から構成される。

【０１００】データ送受信ブロック１６１は、サービスサーバ５４から、ネットワーク２２を介して送信されるコンテンツデータおよびメタデータ、若しくは決済サーバ５８から送信されるコンテンツデータの使用権情報などを受信する。また、データ送受信ブロック１６１は、サービスサーバ５４に対するデータの送信要求、および決済サーバ５８に対する使用権情報を要求する情報などを送信するとともに、データ再生装置１５２に、処理結果を転送する。

【０１０１】コントローラ１６２は、ソフトウエアにより制御され、STB１５１全体の動作を制御する。

【０１０２】暗号化処理ブロック１６３は、データ送受信ブロック１６１が受信するコンテンツデータおよびメタデータの復号関連処理を行う。詳細な構成例については図１３に示す。

【０１０３】フラッシュメモリ１６４は、STB１５１の

電源遮断後もデータを記憶している不揮発性のメモリである。フラッシュメモリ１６４には、各ブロックが処理するために必要なデータ、および各ブロックの処理結果が、適宜、記憶される。

【０１０４】外部RAM１６５は、暗号化処理ブロック１６３による処理結果、および他のブロックが分散処理を行った場合の分散処理結果を記憶する。

【０１０５】図１３は、暗号化処理ブロック１６３の詳細な構成例を示すブロック図である。暗号化処理ブロック１６３は、入出力インタフェースブロック１８１、マイクロプロセッサ１８２、RAM１８３、乱数生成ブロック１８４、フラッシュメモリ１８５、および暗号化処理部１８６より構成される。さらに、暗号化処理部１８６は、暗号化処理サブブロック１８７、ディジタル署名検証サブブロック１８８、およびハッシュ値計算サブブロック１８９より構成される。

【０１０６】入出力インタフェースブロック１８１は、データ送受信ブロック１６１が受信したコンテンツデータおよびメタデータのうち、コントローラ１６２により復号関連処理が必要であると判断され、暗号化処理ブロック１６３に転送されるデータを受信する。入出力インタフェースブロック１８１は、コントローラ１６１から供給されるデータを、マイクロプロセッサ１８２に転送する。マイクロプロセッサ１８２は、暗号化処理ブロック１６３の全体の動作を制御する。

【０１０７】RAM１８３は、マイクロプロセッサ１８２が処理をするのに必要なプログラムを記憶している。また、RAM１８３には、マイクロプロセッサ１８２が処理した結果が記憶される。

【０１０８】乱数生成ブロック１８４は、マイクロプロセッサ１８２からの指令により乱数を生成し、暗号化処理部１８６に供給する。乱数生成ブロック１８４が生成した乱数は、DES、RSAなどの共通鍵暗号方式で暗号関連処理が施されたデータを、復号する場合の鍵として利用される。

【０１０９】フラッシュメモリ１８５は、不揮発性のメモリであり、内部に図示せぬコントローラを保持している。マイクロプロセッサ１８２において動作するソフトウエアの実行コード、復号関連処理に必要となる各種データ、購入したコンテンツデータの使用権情報などが記憶される。

【０１１０】暗号化処理部１８６は、コンテンツデータおよびメタデータの復号関連処理を行う。暗号化処理部１８６は、さらに、以下の機能を提供するサブブロックにより構成される。

【０１１１】暗号化処理サブブロック１８７は、DES、RSAなどの暗号化アルゴリズムにより暗号化されたコンテンツデータの復号処理を行う。

【０１１２】ディジタル署名検証サブブロック１８８は、DSAなどによるディジタル署名アルゴリズムにより

ディジタル署名が付加されたコンテンツデータおよびメタデータのディジタル署名検証処理を行う。

【０１１３】ハッシュ値計算サブブロック１８９は、ハッシュ関数による計算を行う。

【０１１４】図１４は、暗号化処理ブロック１６３が、コントローラ１６２等と送受信するデータ形式の例を示す図である。コントローラ１６２は、暗号化処理ブロック１６３に対して、図１４のデータ形式のコマンドデータで処理を要求する。また、暗号化処理ブロック１６３は、コマンドデータに基づいて各ブロックを制御し、所定の処理を実行させるとともに、コマンドデータにより処理を要求したコントローラ１６２に対して、図１４のデータ形式のレスポンスデータで処理結果を送信する。

【０１１５】フィールド１は、データ種識別フィールドであり、コマンドデータ、またはレスポンスデータの種類が記述される。

【０１１６】フィールド２は、データ番号フィールドであり、コマンドデータ、またはレスポンスデータの番号が記述される。

【０１１７】フィールド３は、データ長フィールドであり、データフィールド４に記述されるデータの長さが記述される。

【０１１８】フィールド４は、データフィールドであり、コマンドデータとして処理を要求するデータ、またはレスポンスデータとして送信する処理結果のデータが記述される。以下、コマンドデータ、およびレスポンスデータの例を説明する。

【０１１９】データ番号フィールドに記述される番号が１であるコマンド１は、ディジタル署名の検証処理の要求を表している。フィールド４のデータフィールドに記述されているデータに対して、暗号化処理ブロック１６３は、データが改竄されていないかを検証し、その処理結果をレスポンス１として、データ処理を要求したブロックに送信する。

【０１２０】コマンド２は、ディジタル署名の生成処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されているデータに対して、ディジタル署名を付加したデータをレスポンス２として、データ処理を要求したブロックに送信する。

【０１２１】コマンド３は、暗号化されているデータの復号処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されている暗号化されているデータに対して、復号処理を行い、復号したデータをレスポンス３として、データ処理を要求したブロックに送信する。

【０１２２】コマンド４は、暗号化処理の要求を表している。暗号化処理ブロック１６３は、フィールド４のデータフィールドに記述されているデータを暗号化し、暗号化したデータをレスポンス４として、データ処理を要

求したブロックに送信する。

【０１２３】コマンド５は、ハッシュ値計算の要求を表している。ハッシュ値計算サブブロック１８９は、フィールド４のデータフィールドに記述されているデータ、およびアルゴリズムをもとに、ハッシュ関数による計算を行い、計算結果のデータをレスポンス５として、データ処理を要求したブロックに送信する。

【０１２４】コマンド６は、処理の停止要求を表している。このコマンドを受信した場合、暗号化処理ブロック１６３は、その時点で行っている処理を停止し、停止した旨の通知をレスポンス６として処理の停止を要求するブロックに送信する。

【０１２５】コマンド７は、使用権情報の送信要求を表している。このコマンドを受信した場合、暗化号処理ブロック１６３は、自らがフラッシュメモリ１８５に保持している使用権情報を暗号化して、決済サーバ５８にレスポンス７として送信する。

【０１２６】コマンド２０は、外部装置または他のブロックから送信されるメッセージである。そのデータフィールドには、コンテンツデータの分散処理先である装置、コントローラ１６２などからメッセージが入力される。

【０１２７】レスポンス３０は、暗号化処理ブロック１６３が、外部装置または他のブロックに対して送信するメッセージである。

【０１２８】以下、コンテンツプロバイダ５１が提供するコンテンツデータを、利用者５５が利用するまでの一連の処理についてフローチャートを参照して説明する。

【０１２９】始めに、図１５のフローチャートを参照して、コンテンツプロバイダ５１が管理するコンテンツサーバ５２の処理を説明する。

【０１３０】ステップS４１において、データキャプチャ装置７１は、ビデオカメラ、およびオーディオレコーダなどから取り込んだアナログデータ、またはディジタルデータを、コンテンツサーバ５２の各装置が処理できるデータ形式に、ディジタル化処理、または圧縮などの処理を行う。

【０１３１】ステップS４２において、データ編集装置７２は、データキャプチャ装置７１から取得したデータから、コンテンツプロバイダ５１の指令に基づいて、利用者５５に提供するコンテンツデータを作成する。また、データ編集装置７２は、メタデータ生成装置７３が生成するメタデータをコンテンツデータに付加する。

【０１３２】図１６は、メタデータ生成装置７３が生成するメタデータの例を示す図である。図１６（A）のメタデータ１の例において、フィールド１には、コンテンツプロバイダ５１を特定するコンテンツプロバイダIDが２、メタデータ１に対応するコンテンツデータ（以下、適宜、コンテンツデータ１と称する。後述する他のメタデータが付加されるコンテンツデータの場合も同様とする）を特定するコンテンツIDが１、コンテンツデータ１の著作権の権利発生日時が西暦２０００年１月１日と記述されている。

【０１３３】フィールド２には、利用者５５によるコンテンツデータ１の利用形態が記述される。ここでは、利用形態１としてストリーミング、利用形態２として買い取りが記述されている。ストリーミングによる利用形態は、利用者端末５６において、サービスサーバ５４からコンテンツデータ１を受信しながらリアルタイムで再生する利用形態であり、利用回数が１回のみの利用形態である。買い取りによる利用形態とは、期間および利用回数が無制限である利用形態であり、利用者端末５６に送信されたコンテンツデータ１は、利用者端末５６の図示せぬ記録媒体に記録される。

【０１３４】フィールド３には、コンテンツデータ１の利用形態毎の料金が記述される。ここでは、コンテンツデータ１を利用形態１のストリーミングにより利用した場合、料金は２０円とされ、コンテンツデータ１を利用形態２の買い取りにより利用した場合、料金は１００円とされている。利用者５５は、フィールド３に記述される料金に基づいて、決済センタ５７に対して使用権情報の代金を支払う。

【０１３５】フィールド４には、コンテンツデータ１の形式的な情報が記述される。ここでは、コンテンツデータ１の総データ量は５７．６MBで、利用者端末５６のデータ再生装置１５２で再生した場合の再生時間は１０分と記述されている。また、コンテンツデータ１は、MP３（MPEG（Moving Picture Experts Group）-1 Audio Layer３）の規格で圧縮されているオーディオデータであり、データ転送速度は１２８Kbpsと記述されている。

【０１３６】フィールド５には、データ暗号化装置７４がコンテンツデータおよびメタデータに施した暗号関連処理の情報が記述される。この例で、ディジタル署名の生成アルゴリズムはDSA、コンテンツデータ１の暗号化アルゴリズムはDES、コンテンツデータ１の暗号化のデータ単位は６４KBと記述されている。暗号化のデータ単位は、１つの暗号化の鍵で連続して暗号化する場合のデータの大きさである。暗号化に利用した鍵はさらに別の鍵（メタ鍵）で暗号化されており、メタ鍵は決済センタ５７に委託され、利用者５５が使用権情報を購入した場合、決済サーバ５８から使用権情報とともに、後述する図２２の使用権情報のデータ形式で、利用者５５に提供される。

【０１３７】図１６（B）のメタデータ２の例において、フィールド１には、コンテンツプロバイダIDが２、コンテンツIDが２、著作権の権利発生日時が西暦２０００年１月１日として記述されている。

【０１３８】フィールド２には、コンテンツデータ２の利用形態１としてストリーミング、利用形態２として買い取り、利用形態３として期間限定１年が記述されてい

る。期間限定１年の利用形態とは、コンテンツデータ２が利用者端末５６の図示せぬ記録媒体に記録された後、利用者５５は期間が１年間以内であれば、回数は無制限にコンテンツデータ２を利用することが可能な形態である。

【０１３９】フィールド３には、コンテンツデータ２の料金が記述されている。料金は、利用形態１のストリーミングにより利用した場合は２０円とされ、利用形態２の買い取りによる利用の場合は１００円とされ、利用形態３の期間限定１年による利用の場合は５０円とされている。

【０１４０】フィールド４には、コンテンツデータ２の総データ量は３００MB、再生時間は１０分と記述されている。また、コンテンツデータ２は、MPEG-２の規格で圧縮されているビデオデータであり、データの転送速度は４Mbpsである。

【０１４１】フィールド５には、ディジタル署名の生成アルゴリズムはDSA、コンテンツデータの暗号化アルゴリズムはDES、暗号化のデータ単位は２５６KBと記述されている。

【０１４２】図１５に戻って、ステップS４３において、データ暗号化装置７４は、データ編集装置７２から転送されるコンテンツデータおよびメタデータに暗号関連処理を施す。

【０１４３】すなわち、乱数生成ブロック９４は、暗号化鍵（コンテンツデータ用）として所定のビット数の乱数を生成し、暗号化処理サブブロック９６に供給する。

【０１４４】暗号化処理サブブロック９６は、乱数生成ブロック９４が生成した乱数を暗号鍵としてコンテンツデータを暗号化するとともに、使用権情報に配置されて決済サーバ５８から利用者端末５６に対して送信されるメタ鍵を使用して、暗号化鍵（コンテンツデータ用）をDESなどの共通鍵暗号方式で暗号化する。

【０１４５】ハッシュ値計算サブブロック９８は、コンテンツサーバ５２がサービスプロバイダ５３に対して送信するメタデータにハッシュ関数を適用してハッシュ値を算出する。

【０１４６】ディジタル署名生成サブブロック９７は、ハッシュ値計算サブブロック９８が抽出したハッシュ値を、乱数生成ブロック９４が生成した乱数よりなる暗号化鍵を利用して暗号化し、ディジタル署名を生成する。

【０１４７】ステップS４４において、データ記憶装置７５は、データ暗号化装置７４により暗号関連処理が施されたデータを記憶し、必要に応じてデータ送信装置７６に出力する。

【０１４８】ステップS４５において、データ送信装置７６は、サービスプロバイダ５３が管理するサービスサーバ５４にメタデータおよびコンテンツデータを送信する。

【０１４９】図１７は、ステップS４５の処理により送信されるデータのフォーマットの例を示す。レイヤ１は、ステップS４２の処理により生成されたメタデータ、ステップS４３の処理により付加されたメタデータ用のディジタル署名、ステップS４３の処理で用いられた暗号化鍵（コンテンツデータ用）、並びにコンテンツデータにより構成される。コンテンツデータは、さらに、レイヤ２としての暗号化単位ブロックにより構成されている。暗号化単位ブロックは、コンテンツデータ１の場合６４KB毎のブロックとされ、コンテンツデータ２の場合２５６KB毎のブロックとされている。

【０１５０】次に、図１８のフローチャートを参照して、サービスプロバイダ５３が管理するサービスサーバ５４の処理を説明する。

【０１５１】ステップS６１において、データ送受信装置１１１は、コンテンツサーバ５２から、暗号関連処理が施されたコンテンツデータおよびメタデータを受信する。

【０１５２】ステップS６２において、メタデータ生成装置１１３は、送信されてきたメタデータを確認し、元のデータを変更し、新たなメタデータを生成する。すなわち、このときデータ暗号化装置１１４は、コンテンツプロバイダ５１から決済サーバ５８を介して予め取得したメタ鍵を利用して、送信されてきた暗号化鍵（コンテンツデータ用）（図１７）を復号し、復号した暗号化鍵（コンテンツデータ用）（図１７）を利用してディジタル署名（メタデータ用）（図１７）を復号する。そして、メタデータ生成装置１１３は、復号して得られたメタデータと、平文で送信されてきたメタデータを比較し、両者が一致していること、すなわち、メタデータが改竄されていないことを確認する。

【０１５３】さらに、メタデータ生成装置１１３は新たにメタデータを生成する。このメタデータは、コンテンツサーバ５２が生成したメタデータ１（図１６（A））およびメタデータ２（図１６（B））のフィールド１およびフィールド３の内容を、サービスプロバイダ５３が利用者５５に通知する情報に書き換えたデータである。メタデータ３およびメタデータ４の内容は、サービスプロバイダ５３が決定する。

【０１５４】図１９は、図１６に示されるコンテンツプロバイダ５１が生成したメタデータを、ステップS６２の処理で、メタデータ生成装置１１３が変更して生成したメタデータの例を示す。図１６（A）のメタデータ１を変更して生成されたメタデータ３（図１９（A））の例においては、フィールド１には、サービスプロバイダ５３を特定するサービスプロバイダIDが２、メタデータ３を作成した日時が西暦２０００年１月２日と記述されている。

【０１５５】フィールド３に記述されている料金には、図１６（A）に示すメタデータ１のフィールド３に記述されている料金に、サービスプロバイダ５３が利用者５

５に対してコンテンツデータを送信する送信料が付加されている。メタデータ３では、料金は、コンテンツデータをストリーミングの利用形態により利用する場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、サービスプロバイダ５３が受け取る送信料の１０円が付加されて３０円とされ、コンテンツデータを買い取りの利用形態により利用する場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、サービスプロバイダ５３が受け取る送信料の５０円が付加されて１５０円とされている。

【０１５６】図１６（Ｂ）のメタデータ２を変更して生成された図１９（Ｂ）のメタデータ４の例においては、フィールド１には、サービスプロバイダIDが２、メタデータ４を作成した日時が西暦２０００年１月２日と記述されている。

【０１５７】フィールド３に記述される料金には、コンテンツデータの利用形態がストリーミングの場合は、コンテンツプロバイダ５１が受け取るコンテンツデータの料金に、送信料の１０円が付加されて３０円とされ、利用形態が買い取りの場合は、送信料の５０円が付加されて１５０円とされ、さらに利用形態が期間限定１年の場合は送信料の３０円が付加されて８０円とされている。

【０１５８】ステップS６３において、データ暗号化装置１１４は、新たに生成したメタデータのハッシュ値を演算し、それを暗号化鍵（コンテンツデータ用）で暗号化し、新たなディジタル署名を生成し、ステップS６２の処理で生成された新たなメタデータに付加する。データ暗号化装置１１４の暗号関連処理は、コンテンツサーバ５２のデータ暗号化装置７４の処理と同様にして行われる。

【０１５９】ステップS６４において、データ編集装置１１２は、サービスサーバ５４の各装置で処理されたデータを編集し、利用者５５に提供するコンテンツデータを作成する。このため、暗号化装置１１４は、送信されてきたコンテンツデータを暗号化鍵（コンテンツデータ用）で一旦復号する。その後データ編集装置１１２により行われる編集には、コンテンツサーバ５２から送信されたコンテンツデータにステップS６２の処理で生成されたメタデータを付加する処理、または複数のコンテンツデータを統合し、１つのコンテンツデータにまとめて利用者５５に提供するアルバム化などの処理がある。編集後のコンテンツデータは、データ暗号化装置１１４により暗号化鍵（コンテンツデータ用）を用いて再び暗号化される。

【０１６０】ステップS６５において、データ記憶装置１１６は、データ編集装置１１２で編集され、データ暗号化装置１１４により暗号化されたデータを記憶する。

【０１６１】ステップS６６において、データ送受信装置１１１は、利用者５５が管理する利用者端末５６から、メタデータの送信が要求されたか否かを判定し、メタデータの送信が要求されたと判定するまで待機する。その後、データ送受信装置１１１が、メタデータの送信が要求されたと判定した場合、処理はステップS６７に進む。

【０１６２】ステップS６７において、データ送受信装置１１１は、利用者５５が要求するコンテンツデータに対応するメタデータを、データ記憶装置１１６から取得し、ネットワーク２２を介して利用者端末５６に送信する。データ送受信装置１１１が送信するメタデータを受信した利用者端末５６のSTB１５１は、メタデータに記述されている内容を確認し、コンテンツデータの復号関連処理の準備をする。STB１５１の詳細な処理については後述するが、その後、STB１５１からコンテンツデータの送信が要求されてくる。

【０１６３】そこで、ステップS６８において、データ送受信装置１１１は、利用者端末５６からコンテンツデータの送信が要求されたか否かを判定する。

【０１６４】データ送受信装置１１１が、利用者端末５６からコンテンツデータの送信が要求されたと判定した場合、処理はステップS６９に進み、データ送受信装置１１１は、データ記憶装置１１６に記憶されているコンテンツデータを、ネットワーク２２を介して利用者端末５６に送信する。

【０１６５】次に、決済センタ５７が管理する決済サーバ５８が、利用者端末５６に対して行うコンテンツデータの使用権情報の発行処理について、図２０および図２１のフローチャートを参照して説明する。

【０１６６】ステップS８１において、ライセンス装置１３２は、利用者端末５６からコンテンツデータの使用権情報の購入が要求されたか否かを判定し、要求されたと判定するまで待機する。ライセンス装置１３２が、利用者端末５６から使用権情報の購入が要求されたと判定した場合、処理はステップS８２に進む。

【０１６７】ステップS８２おいて、ライセンス装置１３２は、使用権情報の購入を要求している利用者５５は、サービスプロバイダ５３からコンテンツデータの提供を受ける契約をしているか否かを確認するため、利用者端末５６のSTB１５１から送信される情報に基づいて、STB１５１は契約対象の機器であるか否かをユーザ管理装置１３３に問い合わせる。この問い合わせに応じて、ユーザ管理装置１３３は、自分自身が管理している契約情報から、使用権情報の購入を要求するSTB１５１は、契約対象の機器であるか否かを検索する。すなわち、このシステムでは、利用者５５はコンテンツデータの提供を受ける前に、サービスプロバイダ５３と予め契約をする必要がある。契約情報は、サービスプロバイダ５３から決済センタ５７に供給され、ユーザ管理装置１３３に登録される。

【０１６８】ステップS８３において、ライセンス装置１３２は、ステップS８２のユーザ管理装置１３３の検

索結果を判定する。ライセンス装置１３２は、使用権情報の購入を要求しているSTB１５１は、契約対象の機器でないと判定した場合、利用者端末５６に対して使用権情報を販売することができないことを通知し、処理を終了する。

【０１６９】ライセンス装置１３２が、使用権情報の購入を要求しているSTB１５１は、契約対象の機器であると判定した場合、処理はステップS８４に進み、ライセンス装置１３２は、データ送受信装置１３１からネットワーク２２を介してSTB１５１の暗号化処理ブロック１６３と相互認証を行い、セッション鍵を共有する。

【０１７０】ステップS８５において、ライセンス装置１３２は、相互認証が成立したか否かを判定し、相互認証が成立していないと判定した場合、処理を終了する。

【０１７１】ステップS８５において、ライセンス装置１３２が、相互認証が成立したと判定した場合、処理はステップS８６に進み、ライセンス装置１３２は、STB１５１から送信される要求内容に基づいて、使用権情報の発行が可能であるか否かを著作権管理装置１３４に問い合わせる。STB１５１から送信される要求内容には、利用者５５が利用を希望するコンテンツデータのコンテンツID、コンテンツデータの利用形態、および使用権情報の代金の決済方法が含まれる。（決済方法がクレジットカードによる決済の場合、クレジットカードのカード番号が、また、決済方法がプリペイドカード型の電子マネーによる決済の場合、プリペイドカードのカード番号が、それぞれ含まれる）このSTB１５１から送信される要求情報は、改竄などの不正処理を防ぐため、暗号化処理ブロック１６３により暗号化されてSTB１５１から送信される。

【０１７２】ステップS８７において、ライセンス装置１３２は、ステップS８６で著作権管理装置１３４に問い合わせた結果を判定する。ライセンス装置１３２は、使用権情報の発行ができないと判定した場合、利用者端末５６に使用権情報の発行ができないことを通知し、処理を終了する。

【０１７３】ステップS８７において、ライセンス装置１３２が、使用権情報の発行が可能であると判定した場合、処理はステップS８８に進み、ライセンス装置１３２は、課金装置１３５に対して課金処理を要求する。

【０１７４】ステップS８９において、課金装置１３５は、自らが管理している料金情報から、利用者５５が要求する使用権情報の代金を取得し、決済装置１３６に対して決済処理の要求をするとともに、利用者端末５６に対して課金情報を通知する。

【０１７５】ステップS９０において、課金装置１３５から決済処理の要求を受けた決済装置１３６は決済処理を行う。決済方法がクレジットカードによる決済の場合、決済装置１３６は、図示せぬクレジットカード会社の決済サーバに、使用権情報の購入を要求している利用者５５のユーザID、および課金装置１３５が取得した使用権情報の代金を通知し、クレジット会社の決済サーバから、決済が可能であるか否かのメッセージを受け取る。決済装置１３６は、メッセージの結果を課金装置１３５に通知する。

【０１７６】利用者５５が要求する決済方法が、プリペイドカード型の電子マネーによる決済の場合、決済装置１３６は、利用者５５から通知されたカードIDと、自分自身が管理するプリペイドカードのカードIDを照合し、決済が可能であるか否かを判定する。決済装置１３６は、この判定結果を課金装置１３５に通知するとともに、決済が可能である場合、利用者５５が使用しているプリペイドカード型の電子マネーの残高情報を更新する。

【０１７７】ステップS９１において、課金装置１３５は、決済装置１３６から通知される情報により、決済が成立したか否かを判定する。決済が成立していないと判定した場合、課金装置１３５は、決済が成立していないことを利用者５５に通知し、処理を終了する。

【０１７８】ステップS９１において、課金装置１３５は、決済が成立したと判定した場合、ライセンス装置１３２に決済が成立したことを通知する。

【０１７９】このときステップS９２において、ライセンス装置１３２は、使用権情報をセッション鍵で暗号化し、ネットワーク２２を介して利用者端末５６に送信する。送信された使用権情報は、STB１５１の暗号化処理ブロック１６３によりセッション鍵で復号される。

【０１８０】図２２は、使用権情報の例を示している。この使用権情報の例では、フィールド１には、利用者５５に対してコンテンツデータの使用権情報の発行を許可するコンテンツプロバイダ５１のIDが２、利用が許可されたコンテンツデータのコンテンツIDが１、および使用権の権利発生日時が西暦２０００年１月２日と記述されている。

【０１８１】フィールド２にはコンテンツプロバイダ５１により許可された利用形態がストリーミングであることが記述されており、フィールド３には、そのストリーミングによる利用形態の料金が３０円とされている。

【０１８２】フィールド４には、メタ鍵が配置されている。通常、利用が許可されたコンテンツデータを復号するための鍵（暗号化鍵（コンテンツデータ用）（図１７））は暗号化されており、メタ鍵はその暗号化鍵（コンテンツデータ用）を復号して取得するための鍵である。

【０１８３】フィールド５には、使用権情報全体のディジタル署名が付加される。

【０１８４】使用権情報は、STB１５１の暗号化処理ブロック１６３により、そのディジタル署名の検証が行われた後、暗号化処理ブロック１６３の内部に配置されているフラッシュメモリ１８５に記憶される。記憶された

使用権情報は、コンテンツデータの復号関連処理において、適宜、利用される。

【０１８５】次に、使用権情報を取得した後のSTB１５１の処理について、図２３乃至図２５のフローチャートを参照して説明する。

【０１８６】ステップS１０１において、利用者５５からの指令に基づいてSTB１５１のコントローラ１６２は、サービスサーバ５４に対して、使用権情報を購入したコンテンツデータに対応するメタデータの送信を要求する。

【０１８７】ステップS１０２において、データ送受信ブロック１６１は、サービスサーバ５４から送信されたメタデータを、ネットワーク２２を介して受信する。

【０１８８】ステップS１０２で受信されたメタデータは、図１９に示すメタデータ３またはメタデータ４である。コントローラ１６２は、メタデータにはディジタル署名が付加されているため、ディジタル署名の検証が必要であると認識する。そこで、コントローラ１６２は、メタデータを暗号化処理ブロック１６３に転送する。

【０１８９】ステップS１０３において、暗号化処理ブロック１６３のマイクロプロセッサ１８２は、転送されてきたメタデータのディジタル署名を検証し、メタデータの正当性を判断する。

【０１９０】すなわち、ハッシュ値計算サブブロック１８９は、平文で送られてきたメタデータにハッシュ関数を適用してハッシュ値を演算する。暗号化処理サブブロック１８７は、フラッシュメモリ１８５に記憶されているメタ鍵で暗号化鍵（コンテンツデータ用）を復号し、さらに、暗号化鍵（コンテンツデータ用）でディジタル署名を復号し、そこに含まれるハッシュ値を得る。ディジタル署名検証サブブロック１８８は、ハッシュ値計算サブブロック１８９が、転送されたメタデータの全文からハッシュ関数を利用して算出したハッシュ値と、暗号化処理サブブロック１８７により復号されたハッシュ値を比較することにより、ディジタル署名を検証する。なお、ハッシュ値計算サブブロック１８９が利用するハッシュ関数は、コンテンツサーバ５２のハッシュ値計算サブブロック９８や、サービスサーバ５４のデータ暗号化装置１１４が利用するハッシュ関数と同一の関数である。

【０１９１】マイクロプロセッサ１８２は、ディジタル署名検証サブブロック１８８が検証した結果を取得し、不正処理の有無を判定する。

【０１９２】ステップS１０４において、マイクロプロセッサ１８２は、メタデータが正常なデータ（改竄されていないデータ）であるか否かを判定し、不正処理を認識した場合（ハッシュ値が一致しない場合）、コントローラ１６２に通知する。コントローラ１６２は、不正処理の存在を利用者５５に通知し、処理を終了する。

【０１９３】ステップS１０４において、マイクロプロセッサ１８２により、メタデータが正常なデータであることが確認された場合、処理はステップS１０５に進み、マイクロプロセッサ１８２は、受信したメタデータの内容を、決済センタ５７から購入し、フラッシュメモリ１８５に記憶されている使用権情報の内容と比較する。これにより、データ送受信ブロック１６１が受信したメタデータは、利用者５５が使用権情報を購入し、サービスサーバ５４に送信を要求するコンテンツデータに対応するメタデータであるか否かがマイクロプロセッサ１８２により判定される。

【０１９４】ステップS１０６において、ステップS１０５でマイクロプロセッサ１８２が比較した結果が、マイクロプロセッサ１８２により判定される。マイクロプロセッサ１８２は、メタデータの内容が、使用権情報の内容と一致せず、正当性が確認できないと判定した場合、コントローラ１６２に通知する。コントローラ１６２は、利用者５５に対してメタデータに不正処理が存在していることを通知し、処理を終了する。

【０１９５】ステップS１０６において、マイクロプロセッサ１８２が、メタデータの内容と使用権情報の内容を比較し、メタデータの正当性を確認した場合、処理はステップS１０７に進む。マイクロプロセッサ１８２は、メタデータに含まれる暗号関連処理情報を確認し、自分自身の復号関連処理の処理能力と比較することにより、コンテンツデータの復号関連処理の準備をする。この例の暗号化処理ブロック１６３は、DESのアルゴリズムで暗号化されているコンテンツデータを復号する機能を有しており、復号関連処理の結果を出力する転送速度は、３Mbpsであるとする。暗号化処理ブロック１６３のこれらの処理能力を基準に、分散処理が必要であるか否かが、ステップS１０８において、マイクロプロセッサ１８２により判定される。

【０１９６】例えば、サービスサーバ５４から送信されるコンテンツデータに、図１９（A）のメタデータ３が対応されている場合のマイクロプロセッサ１８２の処理について説明する。

【０１９７】マイクロプロセッサ１８２は、メタデータ３の内容から、暗号化されているコンテンツデータ３を復号するには、DESのアルゴリズムに対応していることが必要であり、MP３の規格で圧縮されたオーディオデータを、ストリーミングにより再生するには、１２８Kbpsの転送速度の処理能力が要求されていると認識する。ここでマイクロプロセッサ１８２は、自分自身の処理能力と、要求されている処理能力を比較することにより、単独で、コンテンツデータ３を処理することが可能であると判定する。この場合、ステップS１０８において、マイクロプロセッサ１８２は、分散処理が必要でないと判定し、処理はステップS１０９に進む。

【０１９８】ステップS１０９において、マイクロプロセッサ１８２から、暗号化処理ブロック１６３が、単独

でコンテンツデータ３の処理をすることが可能であると通知を受けたコントローラ１６２は、サービスサーバ５４に対してコンテンツデータ３の送信を要求する。

【０１９９】ステップS１１０において、ステップS１０９でコントローラ１６２が要求するコンテンツデータ３は、サービスサーバ５４から送信され、ネットワーク２２を介してデータ送受信ブロック１６１により受信される。コントローラ１６２からコンテンツデータ３の転送を受けた暗号化処理ブロック１６３は、単独で、コンテンツデータ３を復号する。

【０２００】すなわち、暗号化処理ブロック１６３の暗号化処理サブブロック１８７は、フラッシュメモリ１８５に記憶されている使用権情報からメタ鍵を取得し、メタ鍵を利用して、データ送受信ブロック１６１がコンテンツデータ３とともに受信した暗号化鍵（コンテンツデータ３用）を復号する。

【０２０１】暗号化処理サブブロック１８７は、復号して取得した暗号化鍵（コンテンツデータ３用）を利用して暗号化されているコンテンツデータ３を復号する。

【０２０２】次に、サービスサーバ５４から送信されるコンテンツデータに、図１９（B）のメタデータ４が対応されている場合のマイクロプロセッサ１８２の処理について説明する。

【０２０３】マイクロプロセッサ１８２は、メタデータ４に記述されている内容から、DESの暗号化アルゴリズムにより暗号化されたコンテンツデータ４を復号する処理能力が要求され、MPEG２の規格で圧縮されたビデオデータをストリーミングの利用形態により再生する場合、４Mbpsの転送速度が要求されていると認識する。

【０２０４】マイクロプロセッサ１８２は、自分自身の処理能力と、要求される処理能力を比較した結果、暗号化処理ブロック１６３が、単独でコンテンツデータ４を処理することは不可能と認識する。この場合、ステップS１０８において、マイクロプロセッサ１８２は分散処理が必要であると判定し、処理はステップS１１１に進む。

【０２０５】ステップS１１１において、マイクロプロセッサ１８２は、コンテンツデータ４の分散処理が必要であるとコントローラ１６２に通知する。この通知には、コンテンツデータ４の分散処理を行うために必要な情報が含まれる。例えば、コンテンツデータを復号する際に必要なアルゴリズム、暗号化処理ブロック１６３に不足しているデータの処理速度、および分散処理先による復号関連処理の処理結果の出力先などの情報が含まれる。

【０２０６】ステップS１１２において、コントローラ１６２は、マイクロプロセッサ１８２から通知された情報に基づいて、コンテンツデータ４の分散処理先を検索する。分散処理先の候補は、コントローラ１６２にリスト化されて予め与えられおり、この例の場合、ステップS１１３において、コントローラ１６２自身が、コンテンツデータ４の分散処理先として検索される。

【０２０７】ここで、マイクロプロセッサ１８２が要求する処理能力は、コンテンツデータ４のDESによる復号処理結果を２Mbpsで出力、および復号したデータを外部RAM１６５の所定のメモリ領域への転送とする。

【０２０８】ステップS１１４において、コントローラ１６２は、ソフトウエアにより復号処理を行うため、コンテンツデータ４の復号処理の準備としてソフトウエアプロセスを生成する。

【０２０９】ステップS１１５において、コントローラ１６２のソフトウエアプロセスは、マイクロプロセッサ１８２に、コンテンツデータ４の分散処理が可能であると通知する。

【０２１０】ステップS１１６において、マイクロプロセッサ１８２は、ソフトウエアプロセスと相互認証を行い、ステップS１１７で、相互認証が成立したか否かがマイクロプロセッサ１８２により判定される。

【０２１１】ステップS１１７において、マイクロプロセッサ１８２が、ソフトウエアプロセスと相互認証が成立していないと判定した場合、マイクロプロセッサ１８２は、コンテンツデータ４を復号することができないと認識し、コントローラ１６２に相互認証が成立していないと通知する。通知を受け取ったコントローラ１６２は、利用者５５に対して、コンテンツデータ４を復号することができないことを通知し、処理を終了する。

【０２１２】ステップS１１７において、マイクロプロセッサ１８２は、ソフトウエアプロセスと相互認証が成立したと判定した場合、処理はステップS１１８に進み、マイクロプロセッサ１８２は、コンテンツデータ４の分散処理の準備が完了したとコントローラ１６２に通知する。

【０２１３】ステップS１１９において、マイクロプロセッサ１８２からコンテンツデータ４の分散処理の準備が完了したことの通知を受け取ったコントローラ１６２は、サービスサーバ５４に対してコンテンツデータ４の送信を要求する。

【０２１４】ステップS１２０において、データ送受信ブロック１６１は、ネットワーク２２を介してサービスサーバ５４から送信されてくるコンテンツデータ４を受信する。その後、コントローラ１６２は、決定した分散処理形式に基づいて、コンテンツデータ４を暗号化処理ブロック１６３、およびソフトウエアプロセスに対して分配する。

【０２１５】ステップS１２１において、暗号化処理ブロック１６３は、ソフトウエアプロセスに対して、予め指定した分散処理結果の出力先である外部RAM１６５から、ソフトウエアプロセスの処理結果を取得し、自分自身が復号したコンテンツデータ４とともに、データ再生装置１５２に転送する。これにより、利用者５５はコン

テンツデータ４を利用することが可能となる。

【０２１６】以下、コンテンツデータを様々な方式により分散処理する場合のSTB１５１の処理を説明する。なお、暗号化処理ブロック１６３の復号関連処理の処理能力は、上述した例の場合と同様に、DESの暗号化アルゴリズムに対応しており、復号したデータの転送速度は３Mbpsとする。なお、以下の説明において、図２３乃至図２５のフローチャートで、STB１５１が、メタデータ３およびメタデータ４を有するコンテンツデータを受信した場合と同一の処理については、その説明は、適宜、省略する。

【０２１７】STB１５１が受信するデータは、図２６に示すフォーマットで構成されており、サービスサーバ５４のデータ記憶装置１１６に記憶されている。図２６を図１７と比較して明らかなように、この例では、レイヤ２の暗号化単位ブロックはさらに、レイヤ３としての、５１２KBのデータ長のブロックと、ディジタル署名とで構成されている。従って、この例では、この暗号化データに付加されているディジタル署名を検証することにより、コンテンツデータの各暗号化単位ブロックに、改竄などの不正処理が行われているか否かを判断することができる。

【０２１８】次に、STB１５１が、図２７に示すメタデータ５に対応するコンテンツデータ５を受信した場合の処理について説明する。始めに、メタデータ５について説明する。フィールド１には、サービスプロバイダIDが１、コンテンツIDが１、コンテンツデータ５の著作権発生日時が西暦２０００年１月１日として、それぞれ記述されている。

【０２１９】フィールド２には、コンテンツデータ５の利用形態１としてストリーミング、利用形態２として買い取り、利用形態３として期間限定１年が、それぞれ記述されている。

【０２２０】フィールド３には、コンテンツデータ５の料金が、ストリーミングの利用形態によりコンテンツデータ５を利用した場合は３０円と、買い取りの利用形態による利用の場合は１５０円と、期間限定１年の利用形態による利用の場合は８０円と記述されている。

【０２２１】フィールド４には、コンテンツデータ５のデータ再生装置１５２における再生時間は１０分であり、総データ量は２２５MBであると記述されている。また、コンテンツデータ５は、MPEG-２の規格で圧縮されているビデオデータであり、３Mbpsの転送速度が要求されている。

【０２２２】フィールド５には、ディジタル署名の生成アルゴリズムはDSA、コンテンツデータ５の暗号化アルゴリズムはDES、および暗号化のデータ単位は５１２KBであり、暗号化ブロック毎にディジタル署名が付加されていることが記述されている。

【０２２３】マイクロプロセッサ１８２がメタデータ５を受信した場合、マイクロプロセッサ１８２は、メタデータ５に記述されている内容から、データ再生装置１５２において、コンテンツデータ５を再生するために必要なデータ転送速度は３Mbpsであると認識する。そのため、マイクロプロセッサ１８２は、暗号化処理ブロック１６３に要求される処理が復号処理のみである場合、暗号化処理ブロック１６３が、単独で復号処理することが可能であると認識する。ところが、マイクロプロセッサ１８２は、コンテンツデータ５の暗号化ブロックには、ディジタル署名が付加されているため、ディジタル署名の検証処理も要求されていると認識し、単独でコンテンツデータ５を処理することは不可能であると判断する。

【０２２４】上述したメタデータ３および４の場合と同様に、コントローラ１６２自身により、コントローラ１６２のソフトウエアプロセスが分散処理先として検索され、マイクロプロセッサ１８２は、ソフトウエアプロセスに対して、コンテンツデータ５の分散処理を要求する。この場合の要求内容は、５１２KBの暗号化データ毎に付加されているディジタル署名を検証し、不正処理が存在しているか否かを暗号化処理ブロック１６３に通知するものである。

【０２２５】その後、コンテンツデータ５が受信された場合、コンテンツデータ５の復号関連処理は、コントローラ１６２により分配され、暗号化処理ブロック１６３はコンテンツデータ５を復号する。一方、ソフトウエアプロセスはディジタル署名の検証を行う。以上の方法で、コンテンツデータ５の分散処理が達成される。

【０２２６】ソフトウエアプロセスが、ディジタル署名の検証処理において、データの不正処理を検出した場合、暗号化処理ブロック１６３に対して不正処理を検出した旨の通知をするとともに、処理を中止する。

【０２２７】暗号化処理ブロック１６３は、コントローラ１６２から不正処理を検出した旨の通知を受け取った場合、処理の経緯をフラッシュメモリ１８５に記憶して処理を終了する。記憶された処理の経緯は、後日、決済センタ５７に通知され、使用権情報を購入する際に決済された代金が取り消される。

【０２２８】次に、STB１５１が、図２８に示すメタデータ６に対応するコンテンツデータ６を受信した場合の処理について説明する。始めに、メタデータ６について説明する。フィールド１乃至フィールド４の記述は、図２７のメタデータ５と同一であり、その説明は、適宜、省略する。

【０２２９】フィールド５には、ディジタル署名の生成アルゴリズムはDSA、コンテンツデータ６の暗号化アルゴリズムはIDEA(International Data Encryption Algorithm)、暗号化のデータ単位は５１２KBであり、暗号化ブロック毎にディジタル署名が付加されていると記述されている。

【０２３０】マイクロプロセッサ１８２がメタデータ６

を受信した場合、マイクロプロセッサ1-８２は、メタデータ６に記述されている内容から、コンテンツデータ６を復号するためにはIDEAの暗号化アルゴリズムに対応している必要があると認識する。そのため、マイクロプロセッサ１８２は、DESの暗号化アルゴリズムにのみ対応している暗号化処理ブロック１６３が、単独でコンテンツデータ６を復号することは不可能であると認識し、コントローラ１６２のソフトウエアプロセスに復号処理を委託する。

【０２３１】その後、ソフトウエアプロセスによるコンテンツデータ６の復号処理が行われ、コントローラ１６２は、処理結果をデータ再生装置１５２に転送する。

【０２３２】次に、STB１５１が、図２９に示すメタデータ７に対応するコンテンツデータ７を受信した場合のマイクロプロセッサ１８２の処理について説明する。この例においては、暗号化処理ブロック１６３は、コンテンツデータ７の復号処理以外に、他のリアルタイム処理が要求された場合に、分散処理を行うように設定されているとする。また、暗号化処理ブロック１６３は、外部RAM１６５に自由にアクセスすることが可能であるとする。

【０２３３】さらに、マイクロプロセッサ１８２は、内部クロックを有しているとする。内部クロックにより、マイクロプロセッサ１８２は、所定の時間間隔で、分散処理を指令したコントローラ１６２のソフトウエアプロセスによる復号処理が、要求内容に基づいて行われているか否かを判断することができる。始めに、メタデータ７について説明する。フィールド１乃至フィールド３、およびフィールド５の記述は、図２７のメタデータ５と同一であり、その説明は、適宜、省略する。

【０２３４】フィールド４には、コンテンツデータ７の再生時間は１０分であり、総データ量は３００MBであると記述されている。また、コンテンツデータ７はMPEG２の規格で圧縮されているビデオデータであり、２．５Mbpsの転送速度が要求されている。

【０２３５】マイクロプロセッサ１８２は、メタデータ７を受信した場合、メタデータ７に記述されている内容から、データ再生装置１５２においてコンテンツデータ７を再生するために必要なデータ転送速度は２．５Mbpsであると認識する。そのため、暗号化処理ブロック１６３が単独でコンテンツデータ７を復号することは可能であるが、この例における暗号化処理ブロック１６３には、コンテンツデータ７の復号処理以外に、他のリアルタイム処理が要求された場合に、分散処理を行うように設定されている。そのため、暗号化処理ブロック１６３は、暗号化データ毎に付加されているディジタル署名の検証処理が要求されていると認識し、コントローラ１６２のソフトウエアプロセスに対して、コンテンツデータ７の分散処理を要求する。

【０２３６】マイクロプロセッサ１８２は、分散処理の要求とともに、コンテンツデータ７の処理結果を外部RAM１６５の所定のアドレス空間に転送することを指定する。その後、コンテンツデータ７がデータ送受信ブロック１６１により受信された場合、コントローラ１６２のソフトウエアプロセスは、コンテンツデータ７の暗号化データ毎に付加されているディジタル署名を検証する。

【０２３７】マイクロプロセッサ１８２は、自分自身の内部に配置されている内部クロックにより、暗号化処理ブロック１６３の内部処理が、所定時間毎に終了するようにタイムスケジュールを設定することが可能である。マイクロプロセッサ１８２は、その設定により、暗号化処理ブロック１６３の内部処理の空き時間に、外部RAM１６５にアクセスする。ソフトウエアプロセスは、マイクロプロセッサ１８２から外部RAM１６５の所定のアドレス空間に処理結果を転送することを指示されているため、マイクロプロセッサ１８２は、外部RAM１６５の所定のアドレス空間にアクセスすることにより、分散処理によるディジタル署名の検証がソフトウエアプロセスにより、要求に基づいて行われているか否かを判断することが可能となる。

【０２３８】マイクロプロセッサ１８２は、外部RAM１６５の所定のアドレス空間から、ソフトウエアプロセスによるコンテンツデータ７の処理結果が取得できないと認識した場合、または分散処理が要求通りに実行されていないと認識した場合、コントローラ１６２に、分散処理が要求通りに実行されていないことを通知する。その後、コントローラ１６２は処理を終了する。

【０２３９】なお、本発明はディジタルデータを処理する様々な装置に適用可能である。以上の例においては、コンテンツデータの分散処理は、STB１５１の内部に配置されている情報処理部に委託して処理することとしたが、IEEE（The Institute ofElectrical and Electronics Engineer,Inc）１３９４などの通信インタフェースを介してデータを送受信することが可能である場合、外部の装置に配置されている情報処理部に分散処理を委託することもできる。

【０２４０】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータや、STB１５１などに、記録媒体からインストールされる。

【０２４１】図３０は、一連の処理を実行するソフトウェアがインストールされるパーソナルコンピュータ２０１の構成例を示している。パーソナルコンピュータ２０１は、CPU(Central Processing Unit)２１１を内蔵している。CPU２１１にはバス２１４を介して、入出力イン

タフェース２１５が接続されている。入出力インタフェース２１５には、キーボード、マウスなどの入力デバイスよりなる入力部２１６、処理結果としての例えば音声信号を出力する出力部２１７、処理結果としての画像を表示するディスプレイなどよりなる表示部２１８、プログラムや各種データを格納するハードディスクドライブなどよりなる記憶部２１９、LAN(LocalArea Network)やインタネットを介してデータを通信するモデムなどよりなる通信部２２０、および、磁気ディスク２２２（フロッピディスクを含む）、光ディスク２２３（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク２２４（MD(Mini Disc)を含む）、もしくは半導体メモリ２２５などの記録媒体に対してデータを読み書きするドライブ２２１が接続されている。バス２１４には、ROM(Read Only Memory)２１２およびRAM２１３が接続されている。

【０２４２】一連の処理を実行するソフトウェアは、磁気ディスク２２２、光ディスク２２３、光磁気ディスク２２４、および半導体メモリ２２５に格納された状態でパーソナルコンピュータ２０１に供給され、ドライブ２２１によって読み出されて、記憶部２１９に内蔵されるハードディスクドライブにインストールされる。記憶部２１９にインストールされているエージェントプログラムは、入力部２１６に入力されるユーザからのコマンドに対応するCPU２１１の指令によって、記憶部２１９からRAM２１３にロードされて実行される。

【０２４３】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２４４】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０２４５】

【発明の効果】以上のように、本発明の情報処理装置、情報処理方法、および記録媒体のプログラムによれば、コンテンツデータの特徴情報から、コンテンツデータのデータ処理に要求される処理能力を認識し、データ処理に要求される処理能力と、自分自身の処理能力を比較し、自分自身の処理能力が、データ処理に要求される処理能力を充足していない場合、所定のデータ処理部だけでなく、他のデータ処理部とコンテンツデータを分散して処理するようにしたので、低コストで、かつ、機能変更が容易な、迅速にデータを処理することができるシステムを実現することが可能になる。

【図面の簡単な説明】

【図１】従来の復号LSIの構成例を示すブロック図である。

【図２】本発明を適用したデータ処理システムの構成例を示すブロック図である。

【図３】データ送信装置の処理を説明するフローチャートである。

【図４】データ受信装置の処理を説明するフローチャートである。

【図５】データ受信装置の処理を説明する図３の続きのフローチャートである。

【図６】本発明を適用したコンテンツ配信システムの概念を示す図である。

【図７】コンテンツサーバの構成例を示すブロック図である。

【図８】データ暗号化装置の詳細な構成例を示すブロック図である。

【図９】サービスサーバの構成例を示すブロック図である。

【図１０】決済サーバの構成例を示すブロック図である。

【図１１】利用者端末の構成例を示すブロック図である。

【図１２】セットトップボックスの構成例を示すブロック図である。

【図１３】暗号化処理ブロックの詳細な構成例を示すブロック図である。

【図１４】暗号化処理ブロックが送受信するデータ形式の例を示す図である。

【図１５】コンテンツサーバの処理を説明するフローチャートである。

【図１６】コンテンツサーバが生成するメタデータの例を示す図である。

【図１７】コンテンツサーバが送信するデータのフォーマットの例を示す図である。

【図１８】サービスプロバイダの処理を説明するフローチャートである。

【図１９】サービスサーバが生成するメタデータの例を示す図である。

【図２０】決済サーバの使用権情報の発行処理を説明するフローチャートである。

【図２１】決済サーバの使用権情報の発行処理を説明する図１９の続きのフローチャートである。

【図２２】使用権情報の例を示す図である。

【図２３】セットトップボックスの処理を説明するフローチャートである。

【図２４】セットトップボックスの処理を説明する図２２の続きのフローチャートである。

【図２５】セットトップボックスの処理を説明する図２３の続きのフローチャートである。

【図２６】データのフォーマットの例を説明する図である。

【図２７】メタデータの例を示す図である。

【図２８】メタデータの他の例を示す図である。

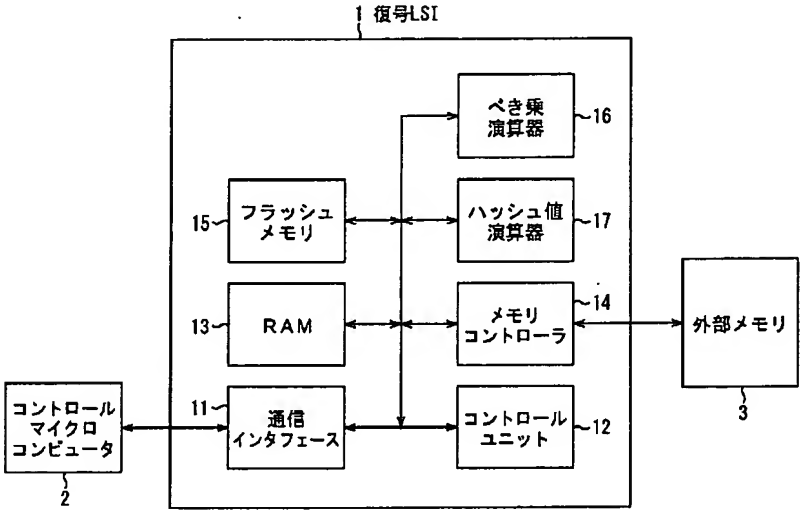
【図２９】メタデータのさらに他の例を示す図である。

【図３０】パーソナルコンピュータの構成例を示すブロック図である。

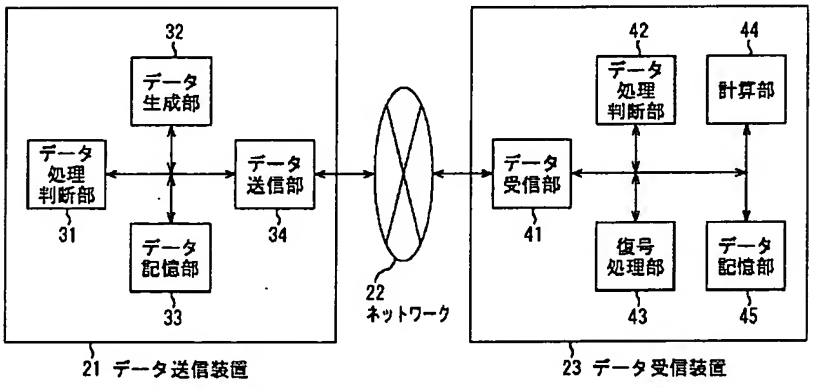
【符号の説明】

２１　データ送信装置，　２２　ネットワーク，　２３　データ受信装置，４１　データ受信部，　４２　データ処理判断部，　４３　復号処理部，　４４計算部，　４５　データ記憶部，　５６　利用者端末，　１５１　セットトップボックス，　１５２　データ再生装置，　＊１６１　データ送受信ブロック，１６２　コントローラ，　１６３　暗号化処理ブロック，　１６４　フラッシュメモリ，　１６５　外部RAM，　１８１　入出力インタフェースブロック，　１８２　マイクロプロセッサ，　１８３　RAM，　１８４　乱数生成ブロック，１８５　フラッシュメモリ，　１８６　暗号化処理部，　１８７　暗号化処理サブブロック，　１８８　ディジタル署名検証サブブロック，　１８９　ハッシュ値計算サブブロック

【図１】



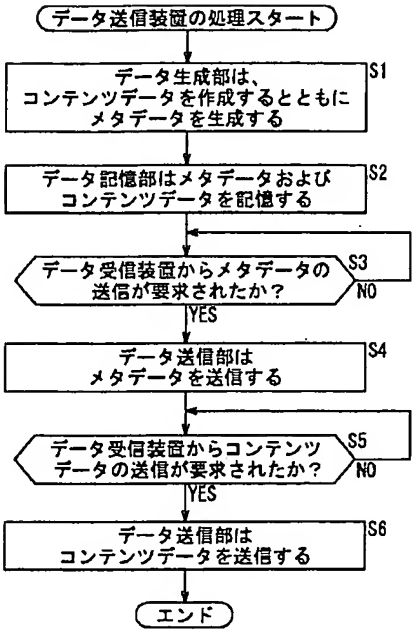
【図２】



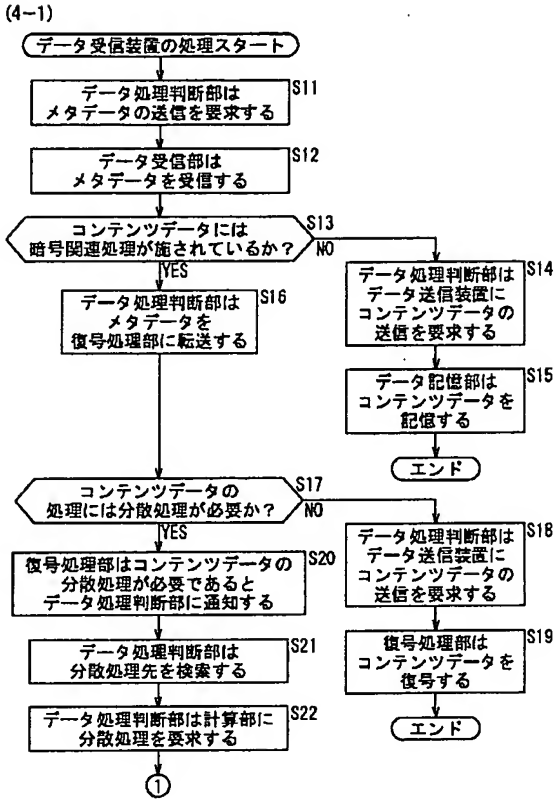
【図１４】

フィールド1	フィールド2	フィールド3	フィールド4
データ種識別フィールド	データ番号フィールド	データ長フィールド	データフィールド

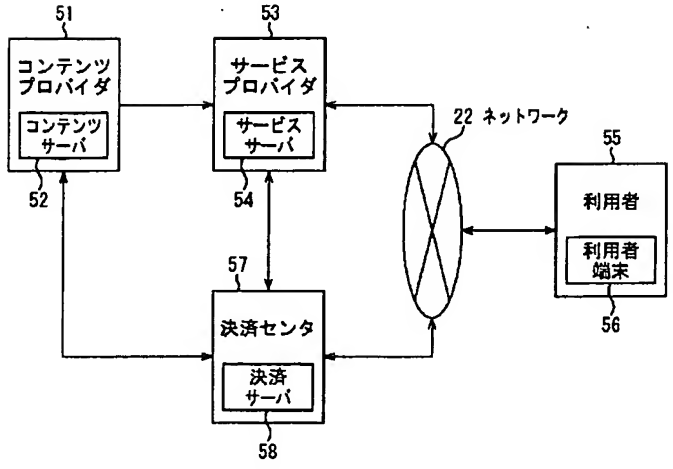
【図３】


データ送信装置の処理スタート
データ生成部は、コンテンツデータを作成するとともにメタデータを生成する
S1
データ記憶部はメタデータおよびコンテンツデータを記憶する
S2
データ受信装置からメタデータの送信が要求されたか？
S3
NO
YES
データ送信部はメタデータを送信する
S4
データ受信装置からコンテンツデータの送信が要求されたか？
S5
NO
YES
データ送信部はコンテンツデータを送信する
S6
エンド

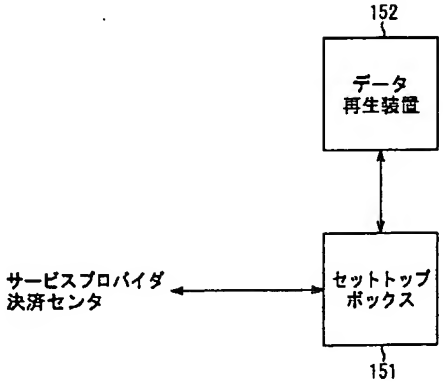
【図４】


(4-1)
データ受信装置の処理スタート
データ処理判断部はメタデータの送信を要求する
S11
データ受信部はメタデータを受信する
S12
コンテンツデータには暗号関連処理が施されているか？
S13
NO
YES
データ処理判断部はメタデータを復号処理部に転送する
S16
データ処理判断部はデータ送信装置にコンテンツデータの送信を要求する
S14
データ記憶部はコンテンツデータを記憶する
S15
エンド
コンテンツデータの処理には分散処理が必要か？
S17
NO
YES
復号処理部はコンテンツデータの分散処理が必要であるとデータ処理判断部に通知する
S20
データ処理判断部は分散処理先を検索する
S21
データ処理判断部は計算部に分散処理を要求する
S22
①
データ処理判断部はデータ送信装置にコンテンツデータの送信を要求する
S18
復号処理部はコンテンツデータを復号する
S19
エンド

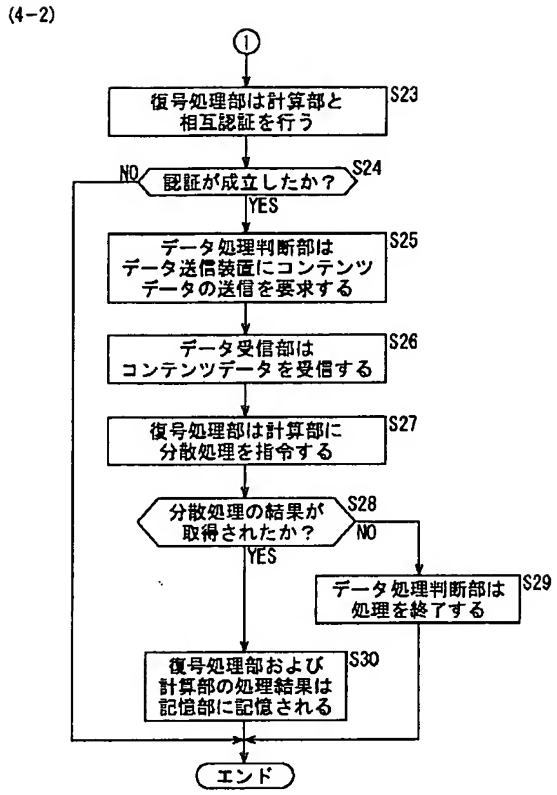
【図６】


51
コンテンツプロバイダ
コンテンツサーバ
52
53
サービスプロバイダ
サービスサーバ
54
22 ネットワーク
55
利用者
利用者端末
56
57
決済センタ
決済サーバ
58

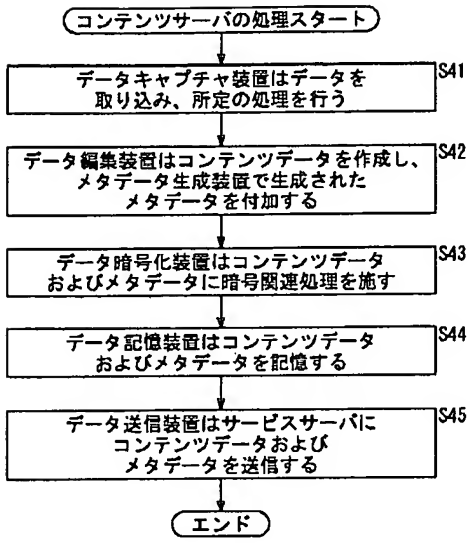
【図１１】


152
データ再生装置
サービスプロバイダ
決済センタ
セットトップボックス
151
利用者端末 56

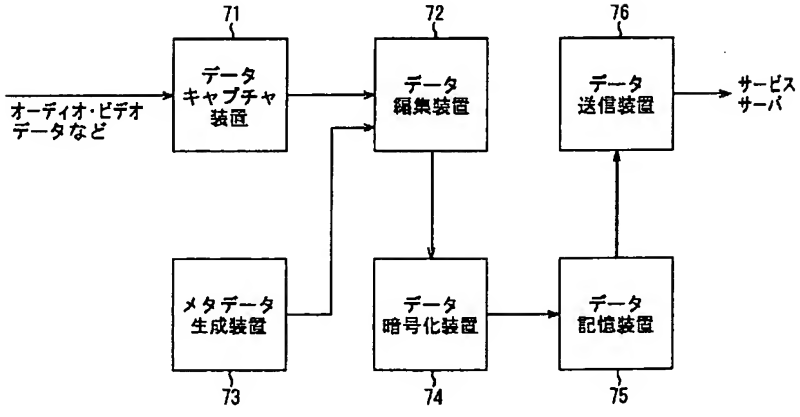
【図５】


(4-2)
①
復号処理部は計算部と相互認証を行う
S23
NO
認証が成立したか？
S24
YES
データ処理判断部はデータ送信装置にコンテンツデータの送信を要求する
S25
データ受信部はコンテンツデータを受信する
S26
復号処理部は計算部に分散処理を指令する
S27
分散処理の結果が取得されたか？
S28
NO
YES
データ処理判断部は処理を終了する
S29
復号処理部および計算部の処理結果は記憶部に記憶される
S30
エンド

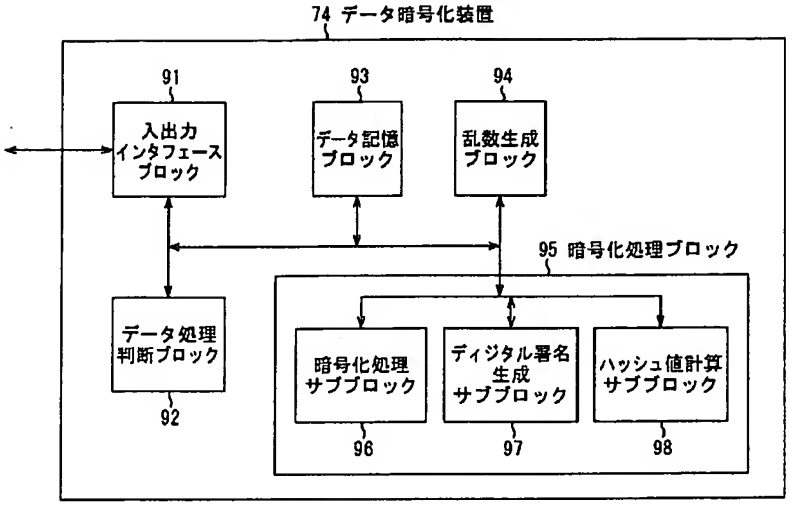
【図１５】


コンテンツサーバの処理スタート
データキャプチャ装置はデータを取り込み、所定の処理を行う
S41
データ編集装置はコンテンツデータを作成し、メタデータ生成装置で生成されたメタデータを付加する
S42
データ暗号化装置はコンテンツデータおよびメタデータに暗号関連処理を施す
S43
データ記憶装置はコンテンツデータおよびメタデータを記憶する
S44
データ送信装置はサービスサーバにコンテンツデータおよびメタデータを送信する
S45
エンド

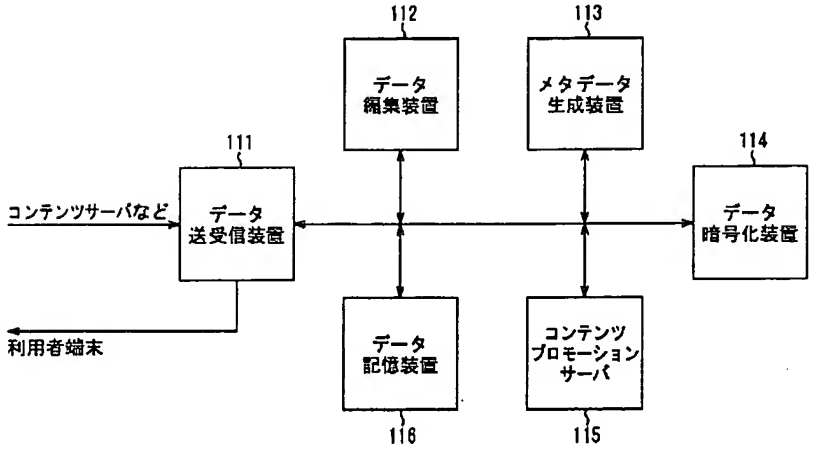
【図７】


71
72
76
データキャプチャ装置
データ編集装置
データ送信装置
オーディオ・ビデオデータなど
サービスサーバ
メタデータ生成装置
データ暗号化装置
データ記憶装置
73
74
75
コンテンツサーバ 52

【図８】

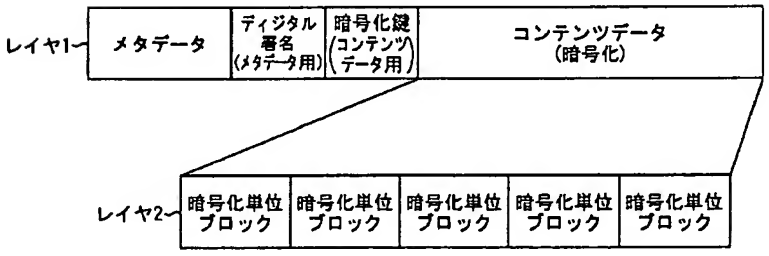


【図９】

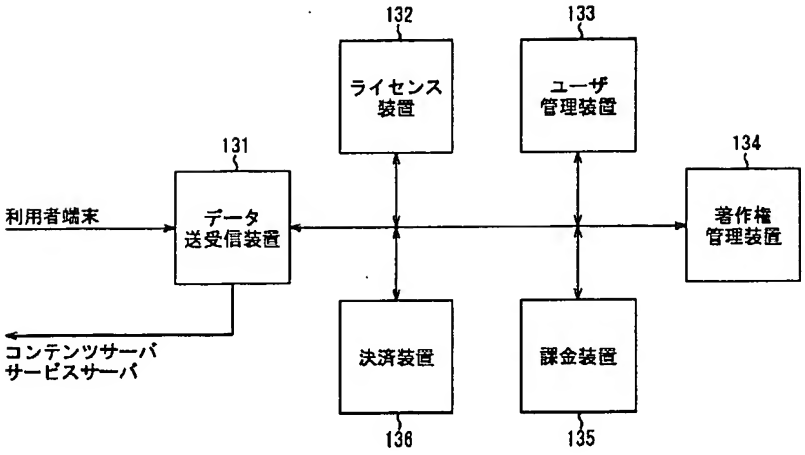


サービスサーバ 54

【図１７】

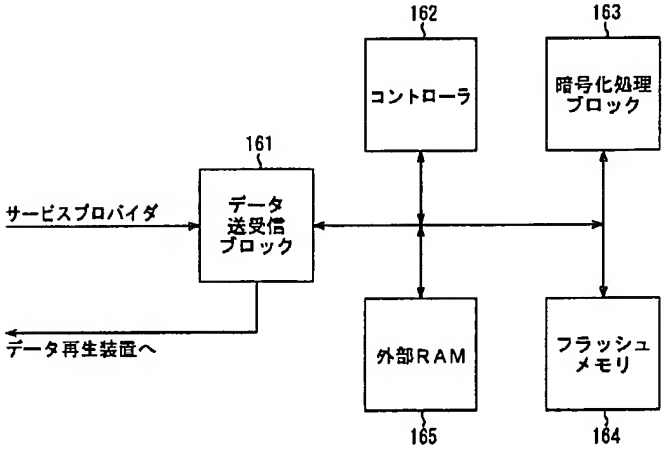


【図１０】



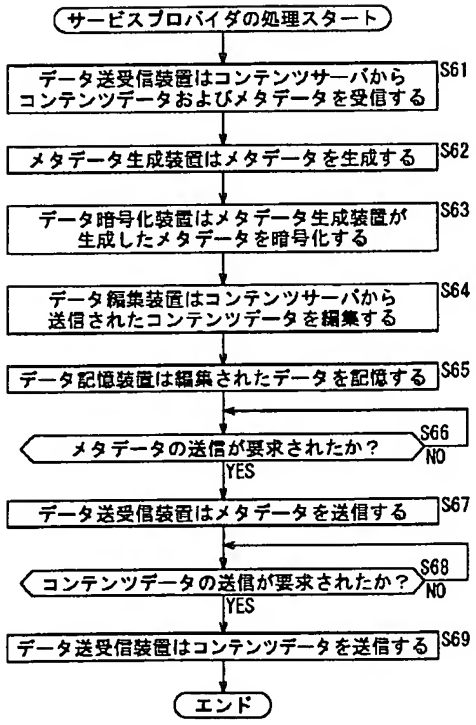
決済サーバ 58

【図１２】

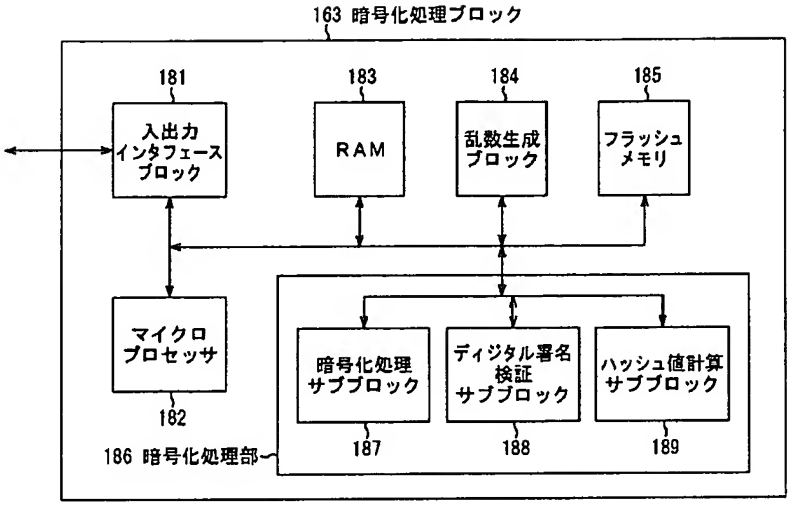


セットトップボックス 151

【図１８】



【図１３】



【図１６】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年1月1日	1 ストリーミング 2 買い取り	1 ¥20 2 ¥100	再生時間 10分 総データ量 57.6MB データ形式 MP3 オーディオデータ 転送速度 128Kbps	ディジタル署名 DSA 暗号化 DES データ単位 64KB

（A）メタデータ1

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 2 権利発生日時 2000年1月1日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥20 2 ¥100 3 ¥50	再生時間 10分 総データ量 300MB データ形式 MPEG2 ビデオデータ 転送速度 4Mbps	ディジタル署名 DSA 暗号化 DES データ単位 256KB

（B）メタデータ2

【図２２】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
コンテンツプロバイダID 2 コンテンツID 1 権利発生日時 2000年1月1日	1 ストリーミング	1 ¥30	メタ鍵	ディジタル署名

【図１９】

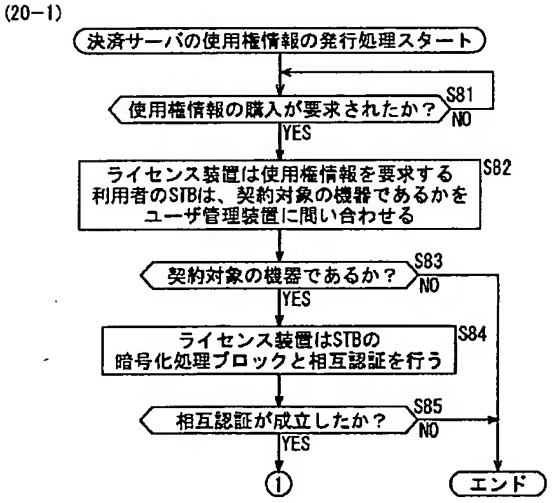
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID　2 コンテンツID メタデータ作成日時　2000年1月2日	1 ストリーミング 2 買い取り	1 ¥30 2 ¥150	再生時間　10分 総データ量　57.6MB データ形式　MP3 オーディオデータ 転送速度　128Kbps	ディジタル署名　DSA 暗号化　DES データ単位　64KB

（A）メタデータ3

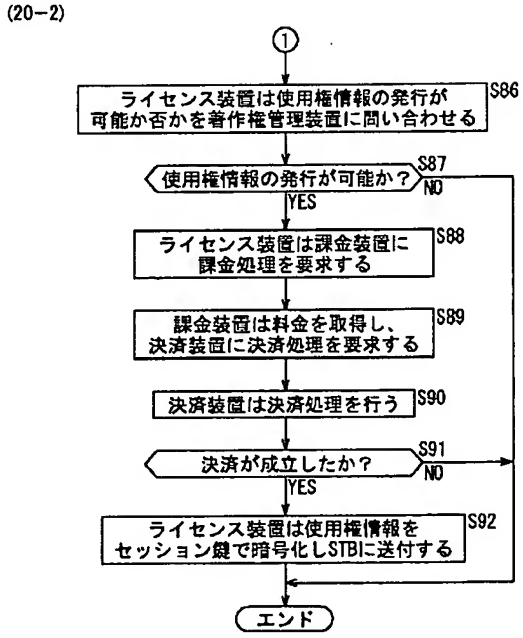
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID　2 コンテンツID　1 メタデータ作成日時　2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間　10分 総データ量　300MB データ形式　MPEG2 ビデオデータ 転送速度　4Mbps	ディジタル署名　DSA 暗号化　DES データ単位　256KB

（B）メタデータ4

【図２０】



【図２１】

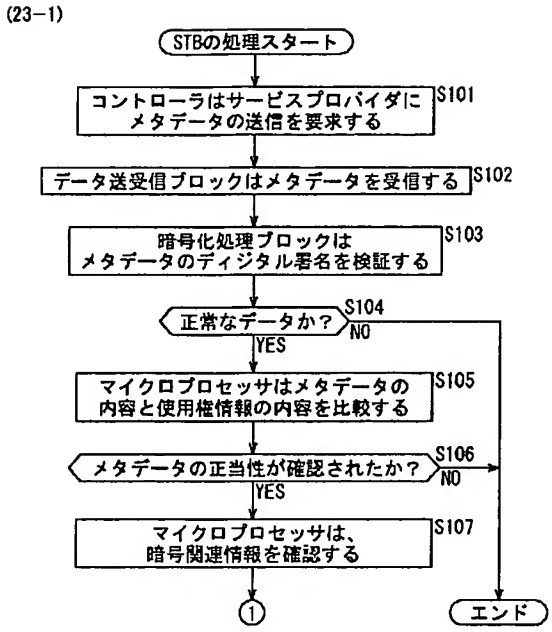


【図２７】

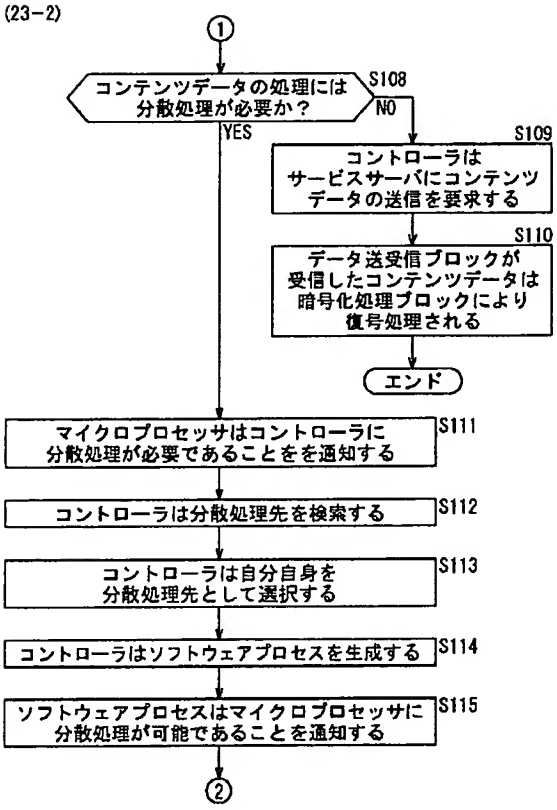
フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID　1 コンテンツID　1 メタデータ作成日時　2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間　10分 総データ量　225MB データ形式　MPEG2 ビデオデータ 転送速度　3Mbps	ディジタル署名　DSA 暗号化　DES データ単位　512KB（署名付）

メタデータ5

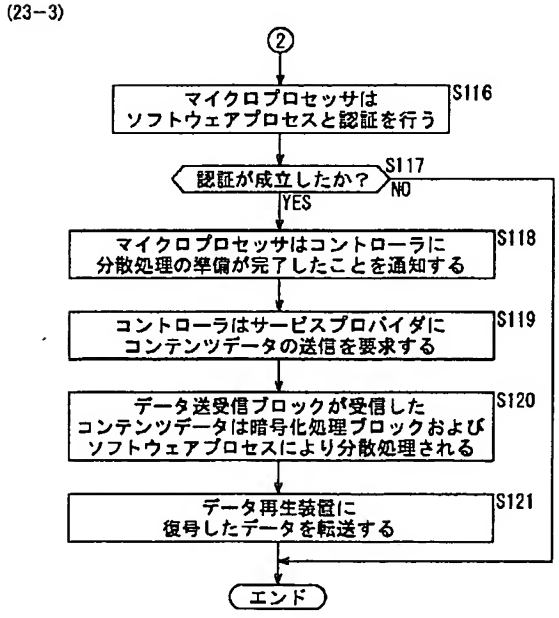
【図２３】


(23-1)
STBの処理スタート
コントローラはサービスプロバイダにメタデータの送信を要求する
S101
データ送受信ブロックはメタデータを受信する
S102
暗号化処理ブロックはメタデータのディジタル署名を検証する
S103
正常なデータか？
S104
NO
YES
マイクロプロセッサはメタデータの内容と使用権情報の内容を比較する
S105
メタデータの正当性が確認されたか？
S106
NO
YES
マイクロプロセッサは、暗号関連情報を確認する
S107
①
エンド

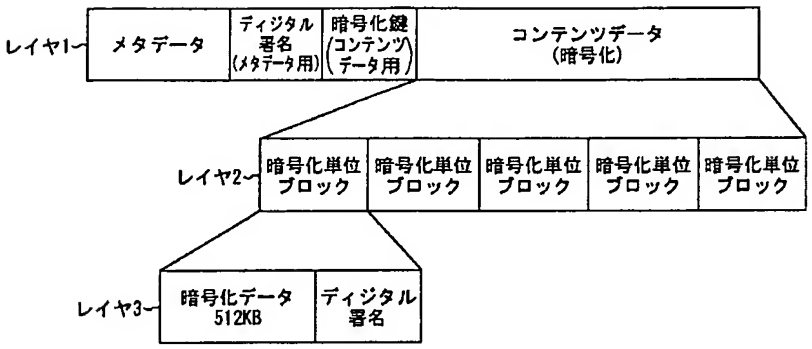
【図２４】


(23-2)
①
コンテンツデータの処理には分散処理が必要か？
S108
NO
YES
コントローラはサービスサーバにコンテンツデータの送信を要求する
S109
データ送受信ブロックが受信したコンテンツデータは暗号化処理ブロックにより復号処理される
S110
エンド
マイクロプロセッサはコントローラに分散処理が必要であることをを通知する
S111
コントローラは分散処理先を検索する
S112
コントローラは自分自身を分散処理先として選択する
S113
コントローラはソフトウェアプロセスを生成する
S114
ソフトウェアプロセスはマイクロプロセッサに分散処理が可能であることを通知する
S115
②

【図２５】


(23-3)
②
マイクロプロセッサはソフトウェアプロセスと認証を行う
S116
認証が成立したか？
S117
NO
YES
マイクロプロセッサはコントローラに分散処理の準備が完了したことを通知する
S118
コントローラはサービスプロバイダにコンテンツデータの送信を要求する
S119
データ送受信ブロックが受信したコンテンツデータは暗号化処理ブロックおよびソフトウェアプロセスにより分散処理される
S120
データ再生装置に復号したデータを転送する
S121
エンド

【図２６】



【図２８】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID　1 コンテンツID　1 メタデータ作成日時　2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間　10分 総データ量　300MB データ形式　MPEG2 ビデオデータ 転送速度　2.5Mbps	ディジタル署名　DSA 暗号化　IDEA データ単位　512KB（署名付）

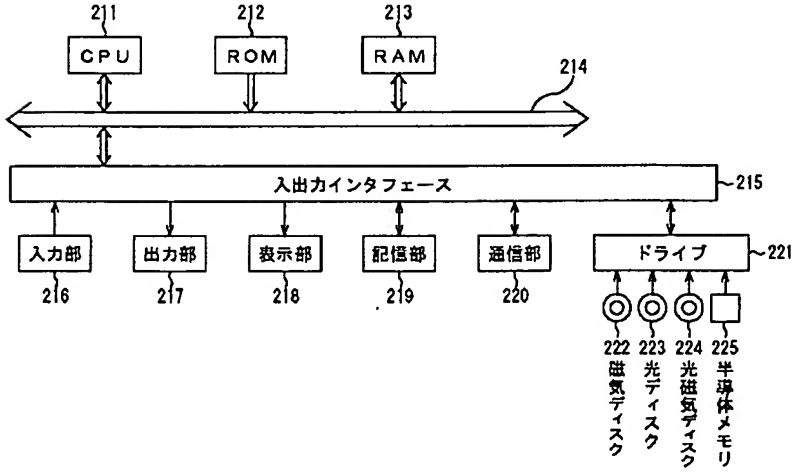
メタデータ6

【図２９】

フィールド1	フィールド2	フィールド3	フィールド4	フィールド5
サービスプロバイダID　1 コンテンツID　1 メタデータ作成日時　2000年1月2日	1 ストリーミング 2 買い取り 3 期間限定1年	1 ¥30 2 ¥150 3 ¥80	再生時間　10分 総データ量　300MB データ形式　MPEG2 ビデオデータ 転送速度　2.5Mbps	ディジタル署名　DSA 暗号化　DES データ単位　512KB（署名付）

メタデータ7

【図３０】



パーソナルコンピュータ 201